SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 05 April 2023

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-47190	Generex UPS CS141 below 2.06 version, could allow a remote attacker to upload a firmware file containing a webshell that could allow him to execute arbitrary code as root.	10.0	More Details
CVE-2023-26968	In Atrocore 1.5.25, the Create Import Feed option with glyphicon-glyphicon-paperclip function is vulnerable to Unauthenticated File upload.	9.8	More Details
CVE-2023-1671	A pre-auth command injection vulnerability in the warn-proceed handler of Sophos Web Appliance older than version 4.3.10.4 allows execution of arbitrary code.	9.8	More Details
CVE-2023-29141	An issue was discovered in MediaWiki before 1.35.10, 1.36.x through 1.38.x before 1.38.6, and 1.39.x before 1.39.3. An auto-block can occur for an untrusted X-Forwarded-For header.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26858	SQL injection vulnerability found in PrestaSHp faqs v.3.1.6 allows a remote attacker to escalate privileges via the faqsBudgetModuleFrontController::displayAjaxGenerateBudget component.	9.8	More Details
CVE-2023-1789	Improper Input Validation in GitHub repository firefly-iii/firefly-iii prior to 6.0.0.	9.8	More Details
CVE-2023-26822	D-Link Go-RT-AC750 revA_v101b03 was discovered to contain a command injection vulnerability via the service parameter at soapcgi.main.	9.8	More Details
CVE-2023-28668	Jenkins Role-based Authorization Strategy Plugin 587.v2872c41fa_e51 and earlier grants permissions even after they've been disabled.	9.8	More Details
CVE-2023-28677	Jenkins Convert To Pipeline Plugin 1.0 and earlier uses basic string concatenation to convert Freestyle projects' Build Environment, Build Steps, and Post-build Actions to the equivalent Pipeline step invocations, allowing attackers able to configure Freestyle projects to prepare a crafted configuration that injects Pipeline script code into the (unsandboxed) Pipeline resulting from a convertion by Jenkins Convert To Pipeline Plugin.	9.8	More Details
CVE-2023-26119	Versions of the package net.sourceforge.htmlunit:htmlunit from 0 and before 3.0.0 are vulnerable to Remote Code Execution (RCE) via XSTL, when browsing the attacker’s webpage.	9.8	More Details
CVE-2023-1765	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Akbim Computer Panon allows SQL Injection.This issue affects Panon: before 1.0.2.	9.8	More Details
CVE-2022-38922	BluePage CMS thru 3.9 processes an insufficiently sanitized HTTP Header Cookie value allowing MySQL Injection in the 'users-cookie-settings' token using a Time-based blind SLEEP payload.	9.8	More Details
CVE-2022-38923	BluePage CMS thru v3.9 processes an insufficiently sanitized HTTP Header allowing MySQL Injection in the 'User-Agent' field using a Time-based blind SLEEP payload.	9.8	More Details
CVE-2023-1728	Unrestricted Upload of File with Dangerous Type vulnerability in Fernus Informatics LMS allows OS Command Injection, Server Side Include (SSI) Injection.This issue affects LMS: before 23.04.03.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26866	GreenPacket OH736's WR-1200 Indoor Unit, OT-235 with firmware versions M-IDU-1.6.0.3_V1.1 and MH-46360-2.0.3-R5-GP respectively are vulnerable to remote command injection. Commands are executed using pre-login execution and executed with root privileges allowing complete takeover.	9.8	More Details
CVE-2023-28879	In Artifex Ghostscript through 10.01.0, there is a buffer overflow leading to potential corruption of data internal to the PostScript interpreter, in base/sbcp.c. This affects BCPEncode, BCPDecode, TBCPEncode, and TBCPDecode. If the write buffer is filled to one byte less than full, and one then tries to write an escaped character, two bytes are written.	9.8	More Details
CVE-2020-19279	Directory Traversal vulnerability found in B3log Wide allows a an attacker to escalate privileges via symbolic links.	9.8	More Details
CVE-2020-19692	Buffer Overflow vulnerabilty found in Nginx NJS v.0feca92 allows a remote attacker to execute arbitrary code via the njs_module_read in the njs_module.c file.	9.8	More Details
CVE-2020-19693	An issue found in Espruino Espruino 6ea4c0a allows an attacker to execute arbitrrary code via oldFunc parameter of the jswrap_object.c:jswrap_function_replacewith endpoint.	9.8	More Details
CVE-2020-19695	Buffer Overflow found in Nginx NJS allows a remote attacker to execute arbitrary code via the njs_object_property parameter of the njs/njs_vm.c function.	9.8	More Details
CVE-2020-20913	SQL Injection vulnerability found in Ming-Soft MCMS v.4.7.2 allows a remote attacker to execute arbitrary code via basic_title parameter.	9.8	More Details
CVE-2020-20914	SQL Injection vulnerability found in San Luan PublicCMS v.4.0 allows a remote attacker to execute arbitrary code via the sql parameter.	9.8	More Details
CVE-2020-20915	SQL Injection vulnerability found in PublicCMS v.4.0 allows a remote attacker to execute arbitrary code via sql parameter of the the SysSiteAdminControl.	9.8	More Details
CVE-2020-29312	An issue found in Zend Framework v.3.1.3 and before allow a remote attacker to execute arbitrary code via the unserialize function. Note: This has been disputed by third parties as incomplete and incorrect. The framework does not have a version that surpasses 2.x.x and was deprecated in early 2020.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28235	Authentication vulnerability found in Etcd-io v.3.4.10 allows remote attackers to escalate privileges via the debug function.	9.8	More Details
CVE-2021-31707	Permissions vulnerability found in KiteCMS allows a remote attacker to execute arbitrary code via the upload file type.	9.8	More Details
CVE-2023-26750	SQL injection vulnerability found in Yii Framework Yii 2 Framework before v.2.0.47 allows the a remote attacker to execute arbitrary code via the runAction function. NOTE: the software maintainer's position is that the vulnerability is in third-party code, not in the framework.	9.8	More Details
CVE-2023-26921	OS Command Injection vulnerability in quectel AG550QCN allows attackers to execute arbitrary commands via ql_atfwd.	9.8	More Details
CVE-2023-23594	An authentication bypass vulnerability in the web client interface for the CL4NX printer before firmware version 1.13.3-u724_r2 provides remote unauthenticated attackers with access to execute commands intended only for valid/authenticated users, such as file uploads and configuration changes.	9.8	More Details
CVE-2023-28843	PrestaShop/paypal is an open source module for the PrestaShop web commerce ecosystem which provides paypal payment support. A SQL injection vulnerability found in the PrestaShop paypal module from release from 3.12.0 to and including 3.16.3 allow a remote attacker to gain privileges, modify data, and potentially affect system availability. The cause of this issue is that SQL queries were being constructed with user input which had not been properly filtered. Only deployments on PrestaShop 1.6 are affected. Users are advised to upgrade to module version 3.16.4. There are no known workarounds for this vulnerability.	9.8	More Details
CVE-2023-28862	An issue was discovered in LemonLDAP::NG before 2.16.1. Weak session ID generation in the AuthBasic handler and incorrect failure handling during a password check allow attackers to bypass 2FA verification. Any plugin that tries to deny session creation after the store step does not deny an AuthBasic session.	9.8	More Details
CVE-2023-28504	Rocket Software UniData versions prior to 8.2.4 build 3003 and UniVerse versions prior to 11.3.5 build 1001 or 12.2.1 build 2002 suffer from a stack-based buffer overflow that can lead to remote code execution as the root user.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2825	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Kepware KEPServerEX 6.11.718.0. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of text encoding conversions. 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 SYSTEM. Was ZDI-CAN-18411.	9.8	More Details
CVE-2022-36972	This vulnerability allows remote attackers to bypass authentication on affected installations of Ivanti Avalanche 6.3.2.3490. The specific flaw exists within the ProfileDaoImpl class. A crafted request can trigger execution of SQL queries composed from a user-supplied string. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-15328.	9.8	More Details
CVE-2022-36974	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ivanti Avalanche 6.3.2.3490. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the Web File Server service. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-15330.	9.8	More Details
CVE-2022-36975	This vulnerability allows remote attackers to bypass authentication on affected installations of Ivanti Avalanche 6.3.2.3490. The specific flaw exists within the ProfileDaoImpl class. A crafted request can trigger execution of SQL queries composed from a user-supplied string. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-15332.	9.8	More Details
CVE-2022-36976	This vulnerability allows remote attackers to bypass authentication on affected installations of Ivanti Avalanche 6.3.2.3490. The specific flaw exists within the GroupDaoImpl class. A crafted request can trigger execution of SQL queries composed from a user-supplied string. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-15333.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36977	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ivanti Avalanche 6.3.2.3490. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the Certificate Management Server service. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-15449.	9.8	More Details
CVE-2022-36978	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ivanti Avalanche 6.3.2.3490. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the Notification Server service. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-15448.	9.8	More Details
CVE-2022-36979	This vulnerability allows remote attackers to bypass authentication on affected installations of Ivanti Avalanche 6.3.2.3490. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the AvalancheDaoSupport class. A crafted request can trigger execution of SQL queries composed from a user-supplied string. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-15493.	9.8	More Details
CVE-2022-36981	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ivanti Avalanche 6.3.3.101. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the DeviceLogResource class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-15966.	9.8	More Details
CVE-2022-36983	This vulnerability allows remote attackers to bypass authentication on affected installations of Ivanti Avalanche. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SetSettings class. 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-15919.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43634	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Netatalk. Authentication is not required to exploit this vulnerability. The specific flaw exists within the dsi_writeinit function. 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 execute code in the context of root. Was ZDI-CAN-17646.	9.8	More Details
CVE-2023-28501	Rocket Software UniData versions prior to 8.2.4 build 3003 and UniVerse versions prior to 11.3.5 build 1001 or 12.2.1 build 2002 suffer from a heap-based buffer overflow in the unirpcd daemon that, if successfully exploited, can lead to remote code execution as the root user.	9.8	More Details
CVE-2023-28502	Rocket Software UniData versions prior to 8.2.4 build 3003 and UniVerse versions prior to 11.3.5 build 1001 or 12.2.1 build 2002 suffer from a stack-based buffer overflow in the "udadmin" service that can lead to remote code execution as the root user.	9.8	More Details
CVE-2023-28503	Rocket Software UniData versions prior to 8.2.4 build 3003 and UniVerse versions prior to 11.3.5 build 1001 or 12.2.1 build 2002 suffer from an authentication bypass vulnerability, where a special username with a deterministic password can be leveraged to bypass authentication checks and execute OS commands as the root user.	9.8	More Details
CVE-2023-28462	A JNDI rebind operation in the default ORB listener in Payara Server 4.1.2.191 (Enterprise), 5.20.0 and newer (Enterprise), and 5.2020.1 and newer (Community), when Java 1.8u181 and earlier is used, allows remote attackers to load malicious code on the server once a JNDI directory scan is performed.	9.8	More Details
CVE-2023-1712	Use of Hard-coded, Security-relevant Constants in GitHub repository deepset-ai/haystack prior to 0.1.30.	9.8	More Details
CVE-2023-28731	AnyMailing Joomla Plugin is vulnerable to unauthenticated remote code execution, when being granted access to the campaign's creation on front-office due to unrestricted file upload allowing PHP code to be injected. This issue affects AnyMailing Joomla Plugin Enterprise in versions below 8.3.0.	9.8	More Details
CVE-2023-1725	Server-Side Request Forgery (SSRF) vulnerability in Infoline Project Management System allows Server Side Request Forgery.This issue affects Project Management System: before 4.09.31.125.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25076	A buffer overflow vulnerability exists in the handling of wildcard backend hosts of SNIProxy 0.6.0-2 and the master branch (commit: 822bb80df9b7b345cc9eba55df74a07b498819ba). A specially crafted HTTP or TLS packet can lead to arbitrary code execution. An attacker could send a malicious packet to trigger this vulnerability.	9.8	More Details
CVE-2023-26829	An authentication bypass vulnerability in the Password Reset component of Gladinet CentreStack before 13.5.9808 allows remote attackers to set a new password for any valid user account, without needing the previous known password, resulting in a full authentication bypass.	9.8	More Details
CVE-2023-28507	Rocket Software UniData versions prior to 8.2.4 build 3003 and UniVerse versions prior to 11.3.5 build 1001 or 12.2.1 build 2002 suffer from a memory-exhaustion issue, where a decompression routine will allocate increasing amounts of memory until all system memory is exhausted and the forked process crashes.	9.8	More Details
CVE-2020-21487	Cross Site Scripting vulnerability found in Netgate pfSense 2.4.4 and ACME package v.0.6.3 allows attackers to execute arbitrary code via the RootFolder field of acme_certificates.php.	9.6	More Details
CVE-2022-42447	HCL Compass is vulnerable to Cross-Origin Resource Sharing (CORS). This vulnerability can allow an unprivileged remote attacker to trick a legitimate user into accessing a special resource and executing a malicious request.	9.6	More Details
CVE-2023-28727	Panasonic AiSEG2 versions 2.00J through 2.93A allows adjacent attackers bypass authentication due to mishandling of X-Forwarded-For headers.	9.6	More Details
CVE-2023-1748	The listed versions of Nexx Smart Home devices use hard-coded credentials. An attacker with unauthenticated access to the Nexx Home mobile application or the affected firmware could view the credentials and access the MQ Telemetry Server (MQTT) server and the ability to remotely control garage doors or smart plugs for any customer.	9.3	More Details
CVE-2023-27162	openapi-generator up to v6.4.0 was discovered to contain a Server-Side Request Forgery (SSRF) via the component /api/gen/clients/{language}. This vulnerability allows attackers to access network resources and sensitive information via a crafted API request.	9.1	More Details
CVE-2023-0344	Akuvox E11 appears to be using a custom version of dropbear SSH server. This server allows an insecure option that by default is not in the official dropbear SSH server.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2848	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Kepware KEPServerEX 6.11.718.0. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of text encoding conversions. 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 SYSTEM. Was ZDI-CAN-16486.	9.1	More Details
CVE-2022-2560	This vulnerability allows remote attackers to delete arbitrary files on affected installations of EnterpriseDT CompleteFTP 22.1.0 Server. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HttpFile class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to delete files in the context of SYSTEM. Was ZDI-CAN-17481.	9.1	More Details
CVE-2023-0432	The web configuration service of the affected device contains an authenticated command injection vulnerability. It can be used to execute system commands on the operating system (OS) from the device in the context of the user "root." If the attacker has credentials for the web service, then the device could be fully compromised.	9.0	More Details
CVE-2023-26482	Nextcloud server is an open source home cloud implementation. In affected versions a missing scope validation allowed users to create workflows which are designed to be only available for administrators. Some workflows are designed to be RCE by invoking defined scripts, in order to generate PDFs, invoking webhooks or running scripts on the server. Due to this combination depending on the available apps the issue can result in a RCE at the end. It is recommended that the Nextcloud Server is upgraded to 24.0.10 or 25.0.4. Users unable to upgrade should disable app `workflow_scripts` and `workflow_pdf_converter` as a mitigation.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2022-42426	This vulnerability allows remote attackers to escalate privileges on affected installations of Centreon. Authentication is required to exploit this vulnerability. The specific flaw exists within the handling of requests to modify poller broker configuration. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to escalate privileges to the level of an administrator. Was ZDI-CAN-18554.	8.8	More Details
CVE-2022-27646	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700v3 1.0.4.120_10.0.91 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the circled daemon. A crafted circleinfo.txt file can trigger an overflow of a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15879.	8.8	More Details
CVE-2022-43636	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of TP-Link TL-WR940N 6_211111 3.20.1(US) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the httpd service, which listens on TCP port 80 by default. The issue results from the lack of sufficient randomness in the sequnce numbers used for session managment. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-18334.	8.8	More Details
CVE-2022-43642	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-825 1.0.9/EE routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the YouTube plugin for the xupnpd service, which listens on TCP port 4044. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the admin user. Was ZDI-CAN-19222.	8.8	More Details
CVE-2022-43643	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-825 1.0.9/EE routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the Generic plugin for the xupnpd service, which listens on TCP port 4044. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the admin user. Was ZDI-CAN-19460.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43644	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-825 1.0.9/EE routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the Dreambox plugin for the xupnpd service, which listens on TCP port 4044. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the admin user. Was ZDI-CAN-19461.	8.8	More Details
CVE-2022-43645	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-825 1.0.9/EE routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the IVI plugin for the xupnpd service, which listens on TCP port 4044. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the admin user. Was ZDI-CAN-19462.	8.8	More Details
CVE-2022-43646	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-825 1.0.9/EE routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the Vimeo plugin for the xupnpd service, which listens on TCP port 4044. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the admin user. Was ZDI-CAN-19463.	8.8	More Details
CVE-2022-27645	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6700v3 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within readycloud_control.cgi. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15762.	8.8	More Details
CVE-2022-43622	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of Login requests to the web management portal. When parsing the HNAP_AUTH header, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16139.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27644	This vulnerability allows network-adjacent attackers to compromise the integrity of downloaded information on affected installations of NETGEAR R6700v3 1.0.4.120_10.0.91 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the downloading of files via HTTPS. The issue results from the lack of proper validation of the certificate presented by the server. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-15797.	8.8	More Details
CVE-2022-27643	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700v3 1.0.4.120_10.0.91 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of SOAP requests. When parsing the SOAPAction header, the process does not properly validate the length of user-supplied data prior to copying it to a buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15692.	8.8	More Details
CVE-2022-27642	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6700v3 1.0.4.120_10.0.91 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the httpd service. The issue results from incorrect string matching logic when accessing protected pages. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-15854.	8.8	More Details
CVE-2022-27641	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700v3 1.0.4.120_10.0.91 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the NetUSB 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-15806.	8.8	More Details
CVE-2022-43647	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-825 1.0.9/EE routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the xupnpd service, which listens on TCP port 4044. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the admin user. Was ZDI-CAN-19464.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36971	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ivanti Avalanche 6.3.2.3490. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the JwtTokenUtility class. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-15301.	8.8	More Details
CVE-2022-43630	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of http requests to the web management portal. When parsing the SOAPAction header, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16150.	8.8	More Details
CVE-2022-43621	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-1935 1.03 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from an incorrectly implemented comparison. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-16152.	8.8	More Details
CVE-2023-0189	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer handler which may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	8.8	More Details
CVE-2022-42427	This vulnerability allows remote attackers to escalate privileges on affected installations of Centreon. Authentication is required to exploit this vulnerability. The specific flaw exists within the contact groups configuration page. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to escalate privileges to the level of an administrator. Was ZDI-CAN-18541.	8.8	More Details
CVE-2023-28676	A cross-site request forgery (CSRF) vulnerability in Jenkins Convert To Pipeline Plugin 1.0 and earlier allows attackers to create a Pipeline based on a Freestyle project, potentially leading to remote code execution (RCE).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28674	A cross-site request forgery (CSRF) vulnerability in Jenkins OctoPerf Load Testing Plugin Plugin 4.5.2 and earlier allows attackers to connect to a previously configured Octoperf server using attacker-specified credentials.	8.8	More Details
CVE-2023-20559	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	8.8	More Details
CVE-2022-3210	This vulnerability allows network-adjacent attackers to execute arbitrary commands on affected installations of D-Link DIR-2150 4.0.1 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the xupnpd service, which listens on TCP port 4044 by default. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-15905.	8.8	More Details
CVE-2022-42424	This vulnerability allows remote attackers to escalate privileges on affected installations of Centreon. Authentication is required to exploit this vulnerability. The specific flaw exists within the handling of requests to modify poller broker configuration. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to escalate privileges to the level of an administrator. Was ZDI-CAN-18556.	8.8	More Details
CVE-2022-42425	This vulnerability allows remote attackers to escalate privileges on affected installations of Centreon. Authentication is required to exploit this vulnerability. The specific flaw exists within the handling of requests to modify poller broker configuration. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to escalate privileges to the level of an administrator. Was ZDI-CAN-18555.	8.8	More Details
CVE-2022-42428	This vulnerability allows remote attackers to escalate privileges on affected installations of Centreon. Authentication is required to exploit this vulnerability. The specific flaw exists within the handling of requests to modify poller broker configuration. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to escalate privileges to the level of an administrator. Was ZDI-CAN-18410.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43620	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-1935 1.03 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper implementation of the authentication algorithm. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-16142.	8.8	More Details
CVE-2020-21514	An issue was discovered in Fluent Fluentd v.1.8.0 and Fluent-ui v.1.2.2 allows attackers to gain escalated privileges and execute arbitrary code due to a default password.	8.8	More Details
CVE-2020-21060	SQL injection vulnerability found in PHPMyWind v.5.6 allows a remote attacker to gain privileges via the delete function of the administrator management page.	8.8	More Details
CVE-2022-42429	This vulnerability allows remote attackers to escalate privileges on affected installations of Centreon. Authentication is required to exploit this vulnerability. The specific flaw exists within the handling of requests to modify poller broker configuration. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to escalate privileges to the level of an administrator. Was ZDI-CAN-18557.	8.8	More Details
CVE-2023-1820	Heap buffer overflow in Browser History in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2022-43608	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Canon imageCLASS MF644Cdw 10.03 printers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the BJNP service. 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-16032.	8.8	More Details
CVE-2023-20558	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43648	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 1.20B03 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the MiniDLNA service. 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 MiniDLNA service. Was ZDI-CAN-19910.	8.8	More Details
CVE-2023-0820	The User Role by BestWebSoft WordPress plugin before 1.6.7 does not protect against CSRF in requests to update role capabilities, leading to arbitrary privilege escalation of any role.	8.8	More Details
CVE-2022-47542	Red Gate SQL Monitor 11.0.14 through 12.1.46 has Incorrect Access Control, exploitable remotely for Escalation of Privileges.	8.8	More Details
CVE-2022-47192	Generex UPS CS141 below 2.06 version, could allow a remote attacker to upload a backup file containing a modified "users.json" to the web server of the device, allowing him to replace the administrator password.	8.8	More Details
CVE-2023-25356	CoreDial sipXcom up to and including 21.04 is vulnerable to Improper Neutralization of Argument Delimiters in a Command. XMPP users are able to inject arbitrary arguments into a system command, which can be used to read files from, and write files to, the sipXcom server. This can also be leveraged to gain remote command execution.	8.8	More Details
CVE-2023-25355	CoreDial sipXcom up to and including 21.04 is vulnerable to Insecure Permissions. A user who has the ability to run commands as the `daemon` user on a sipXcom server can overwrite a service file, and escalate their privileges to `root`.	8.8	More Details
CVE-2023-1762	Improper Privilege Management in GitHub repository thorsten/phpmyfaq prior to 3.1.12.	8.8	More Details
CVE-2023-0480	VitalPBX version 3.2.3-8 allows an unauthenticated external attacker to obtain the instance administrator's account. This is possible because the application is vulnerable to CSRF.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29003	SvelteKit is a web development framework. The SvelteKit framework offers developers an option to create simple REST APIs. This is done by defining a `+server.js` file, containing endpoint handlers for different HTTP methods. SvelteKit provides out-of-the-box cross-site request forgery (CSRF) protection to its users. While the implementation does a sufficient job in mitigating common CSRF attacks, prior to version 1.15.1, the protection can be bypassed by simply specifying a different `Content-Type` header value. If abused, this issue will allow malicious requests to be submitted from third-party domains, which can allow execution of operations within the context of the victim's session, and in extreme scenarios can lead to unauthorized access to users' accounts. SvelteKit 1.15.1 updates the `is_form_content_type` function call in the CSRF protection logic to include `text/plain`. As additional hardening of the CSRF protection mechanism against potential method overrides, SvelteKit 1.15.1 is now performing validation on `PUT`, `PATCH` and `DELETE` methods as well. This latter hardening is only needed to protect users who have put in some sort of `?_method= override` feature themselves in their `handle` hook, so that the request that resolve sees could be `PUT`/`PATCH`/`DELETE` when the browser issues a `POST` request.	8.8	More Details
CVE-2023-0213	Elevation of privilege issue in M-Files Installer versions before 22.6 on Windows allows user to gain SYSTEM privileges via DLL hijacking.	8.8	More Details
CVE-2023-1509	The GMAce plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.5.2. This is due to missing nonce validation on the gmace_manager_server function called via the wp_ajax_gmace_manager AJAX action. This makes it possible for unauthenticated attackers to modify arbitrary files and achieve remote code execution via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2023-27534	A path traversal vulnerability exists in curl <8.0.0 SFTP implementation causes the tilde (~) character to be wrongly replaced when used as a prefix in the first path element, in addition to its intended use as the first element to indicate a path relative to the user's home directory. Attackers can exploit this flaw to bypass filtering or execute arbitrary code by crafting a path like /~2/foo while accessing a server with a specific user.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27533	A vulnerability in input validation exists in curl <8.0 during communication using the TELNET protocol may allow an attacker to pass on maliciously crafted user name and "telnet options" during server negotiation. The lack of proper input scrubbing allows an attacker to send content or perform option negotiation without the application's intent. This vulnerability could be exploited if an application allows user input, thereby enabling attackers to execute arbitrary code on the system.	8.8	More Details
CVE-2023-0265	Uvdesk version 1.1.1 allows an authenticated remote attacker to execute commands on the server. This is possible because the application does not properly validate profile pictures uploaded by customers.	8.8	More Details
CVE-2023-1810	Heap buffer overflow in Visuals in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-1811	Use after free in Frames in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-1812	Out of bounds memory access in DOM Bindings in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2022-36973	This vulnerability allows remote attackers to bypass authentication on affected installations of Ivanti Avalanche 6.3.2.3490. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the ProfileDaoImpl class. A crafted request can trigger execution of SQL queries composed from a user-supplied string. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-15329.	8.8	More Details
CVE-2023-28935	** UNSUPPORTED WHEN ASSIGNED ** Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Apache Software Foundation Apache UIMA DUCC. When using the "Distributed UIMA Cluster Computing" (DUCC) module of Apache UIMA, an authenticated user that has the permissions to modify core entities can cause command execution as the system user that runs the web process. As the "Distributed UIMA Cluster Computing" module for UIMA is retired, we do not plan to release a fix for this issue. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43940	Hitachi Vantara Pentaho Business Analytics Server versions before 9.4.0.1 and 9.3.0.2, including 8.3.x do not correctly perform an authorization check in the data source management service.	8.8	More Details
CVE-2023-28505	Rocket Software UniData versions prior to 8.2.4 build 3003 and UniVerse versions prior to 11.3.5 build 1001 or 12.2.1 build 2002 suffer from a buffer overflow in an API function, where a string is copied into a caller-provided buffer without checking the length. This requires a valid login to exploit.	8.8	More Details
CVE-2022-43769	Hitachi Vantara Pentaho Business Analytics Server prior to versions 9.4.0.1 and 9.3.0.2, including 8.3.x allow certain web services to set property values which contain Spring templates that are interpreted downstream.	8.8	More Details
CVE-2022-43773	Hitachi Vantara Pentaho Business Analytics Server prior to versions 9.4.0.1 and 9.3.0.2, including 8.3.x is installed with a sample HSQLDB data source configured with stored procedures enabled.	8.8	More Details
CVE-2022-43938	Hitachi Vantara Pentaho Business Analytics Server prior to versions 9.4.0.1 and 9.3.0.2, including 8.3.x cannot allow a system administrator to disable scripting capabilities of Pentaho Reports (*.prpt) through the JVM script manager.	8.8	More Details
CVE-2023-28508	Rocket Software UniData versions prior to 8.2.4 build 3003 and UniVerse versions prior to 11.3.5 build 1001 or 12.2.1 build 2002 suffer from a heap-based overflow vulnerability, where certain input can corrupt the heap and crash the forked process.	8.8	More Details
CVE-2023-28506	Rocket Software UniData versions prior to 8.2.4 build 3003 and UniVerse versions prior to 11.3.5 build 1001 or 12.2.1 build 2002 suffer from a stack-based buffer overflow, where a string is copied into a buffer using a memcpy-like function and a user-provided length. This requires a valid login to exploit.	8.8	More Details
CVE-2023-1818	Use after free in Vulkan in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2020-19278	Cross Site Request Forgery vulnerability found in Phachon mm-wiki v.0.1.2 allows a remote attacker to execute arbitrary code via the system/user/save parameter.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1815	Use after free in Networking APIs in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2022-43939	Hitachi Vantara Pentaho Business Analytics Server versions before 9.4.0.1 and 9.3.0.2, including 8.3.x contain security restrictions using non-canonical URLs which can be circumvented.	8.6	More Details
CVE-2022-23522	MindsDB is an open source machine learning platform. An unsafe extraction is being performed using `shutil.unpack_archive()` from a remotely retrieved tarball. Which may lead to the writing of the extracted files to an unintended location. This vulnerability is sometimes called a **TarSlip** or a **ZipSlip variant**. Unpacking files using the high-level function `shutil.unpack_archive()` from a potentially malicious tarball without validating that the destination file path remained within the intended destination directory may cause files to be overwritten outside the destination directory. An attacker could craft a malicious tarball with a filename path, such as `../../../../../../../../etc/passwd`, and then serve the archive remotely using a personal bucket `s3`, thus, retrieve the tarball through **mindsdb** and overwrite the system files of the hosting server. This issue has been addressed in version 22.11.4.3. Users are advised to upgrade. Users unable to upgrade should avoid ingesting archives from untrusted sources.	8.5	More Details
CVE-2023-0208	NVIDIA DCGM for Linux contains a vulnerability in HostEngine (server component) where a user may cause a heap-based buffer overflow through the bound socket. A successful exploit of this vulnerability may lead to denial of service and data tampering.	8.4	More Details
CVE-2023-27286	IBM Aspera Cargo 4.2.5 and IBM Aspera Connect 4.2.5 are vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow a buffer and execute arbitrary code on the system. IBM X-Force ID: 248616.	8.4	More Details
CVE-2023-27284	IBM Aspera Cargo 4.2.5 and IBM Aspera Connect 4.2.5 are vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow a buffer and execute arbitrary code on the system. IBM X-Force ID: 248616.	8.4	More Details
CVE-2023-27089	Cross Site Scripting vulnerability found in Ehuacui BBS allows attackers to cause a denial of service via a crafted payload in the login parameter.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27487	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, the client may bypass JSON Web Token (JWT) checks and forge fake original paths. The header `x-envoy-original-path` should be an internal header, but Envoy does not remove this header from the request at the beginning of request processing when it is sent from an untrusted client. The faked header would then be used for trace logs and grpc logs, as well as used in the URL used for `jwt_authn` checks if the `jwt_authn` filter is used, and any other upstream use of the x-envoy-original-path header. Attackers may forge a trusted `x-envoy-original-path` header. Versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9 have patches for this issue.	8.2	More Details
CVE-2022-45355	Auth. (admin+) SQL Injection (SQLi) vulnerability in ThimPress WP Pipes plugin <= 1.33 versions.	8.2	More Details
CVE-2023-0835	markdown-pdf version 11.0.0 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not validate the Markdown content entered by the user.	8.2	More Details
CVE-2023-28681	Jenkins Visual Studio Code Metrics Plugin 1.7 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	8.2	More Details
CVE-2023-28682	Jenkins Performance Publisher Plugin 8.09 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	8.2	More Details
CVE-2023-28683	Jenkins Phabricator Differential Plugin 2.1.5 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	8.2	More Details
CVE-2023-0975	A vulnerability exists in Trellix Agent for Windows version 5.7.8 and earlier, that allows local users, during install/upgrade workflow, to replace one of the Agent’s executables before it can be executed. This allows the user to elevate their permissions.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27493	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, Envoy does not sanitize or escape request properties when generating request headers. This can lead to characters that are illegal in header values to be sent to the upstream service. In the worst case, it can cause upstream service to interpret the original request as two pipelined requests, possibly bypassing the intent of Envoy's security policy. Versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9 contain a patch. As a workaround, disable adding request headers based on the downstream request properties, such as downstream certificate properties.	8.1	More Details
CVE-2022-36980	This vulnerability allows remote attackers to bypass authentication on affected installations of Ivanti Avalanche 6.3.2.3490. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the EnterpriseServer service. The issue results from the lack of proper locking when performing operations during authentication. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-15528.	8.1	More Details
CVE-2023-1752	The listed versions of Nexx Smart Home devices could allow any user to register an already registered alarm or associated device with only the device's MAC address.	8.1	More Details
CVE-2023-26984	An issue in the password reset function of Peppermint v0.2.4 allows attackers to access the emails and passwords of the Tickets page via a crafted request.	8.1	More Details
CVE-2022-48434	libavcodec/pthread_frame.c in FFmpeg before 5.1.2, as used in VLC and other products, leaves stale hwaccel state in worker threads, which allows attackers to trigger a use-after-free and execute arbitrary code in some circumstances (e.g., hardware re-initialization upon a mid-video SPS change when Direct3D11 is used).	8.1	More Details
CVE-2022-42433	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link TL-WR841N TL-WR841N(US)_V14_220121 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the ated_tp service. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-17356.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27647	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700v3 1.0.4.120_10.0.91 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of the name or email field provided to libreadycloud.so. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15874.	8.0	More Details
CVE-2023-28854	nophp is a PHP web framework. Prior to version 0.0.1, nophp is vulnerable to shell command injection on httpd user. A patch was made available at commit e5409aa2d441789cbb35f6b119bef97ecc3986aa on 2023-03-30. Users should update index.php to 2023-03-30 or later or, as a workaround, add a function such as `env_patchsample230330.php` to env.php.	8.0	More Details
CVE-2022-28687	This vulnerability allows remote attackers to execute arbitrary code on affected installations of AVEVA Edge 2020 SP2 Patch 0(4201.2111.1802.0000). 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 APP files. The process loads a library from an unsecured location. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16257.	7.8	More Details
CVE-2022-28303	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.16.02.022. 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 SKP 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-16280.	7.8	More Details
CVE-2022-27648	This vulnerability allows remote attackers to execute arbitrary code on affected installations of KOYO Screen Creator 0.1.1.1. 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 SCA2 files. 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 the current process. Was ZDI-CAN-14868.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28300	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation 10.16.02.034 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 JP2 images. Crafted data in a JP2 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-16202.	7.8	More Details
CVE-2022-28301	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.34. 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 IFC files. Crafted data in an IFC 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-16392.	7.8	More Details
CVE-2022-28302	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.34. 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 IFC files. Crafted data in an IFC file can trigger a read past the end of an allocated buffer. An attacker can leverage this to execute code in the context of the current process. Was ZDI-CAN-16446.	7.8	More Details
CVE-2022-28688	This vulnerability allows remote attackers to execute arbitrary code on affected installations of AVEVA Edge 2020 SP2 Patch 0(4201.2111.1802.0000). 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 APP files. The process loads a library from an unsecured location. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-17201.	7.8	More Details
CVE-2023-26991	SWFTools v0.9.2 was discovered to contain a stack-use-after-scope in the swf_ReadSWF2 function in lib/rfxswf.c.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43639	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 12.0.1.12430. 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 U3D 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-18628.	7.8	More Details
CVE-2022-43638	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 12.0.1.12430. 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 U3D 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-18627.	7.8	More Details
CVE-2022-43637	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 12.0.1.12430. 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 U3D 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-18626.	7.8	More Details
CVE-2022-28304	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.034. 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 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 the current process. Was ZDI-CAN-16171.	7.8	More Details
CVE-2023-27759	An issue found in Wondershare Technology Co, Ltd Edrawmind v.10.0.6 allows a remote attacker to executea arbitrary commands via the WindowsCodescs.dll file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28305	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.034. 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 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 the current process. Was ZDI-CAN-16172.	7.8	More Details
CVE-2022-28306	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.034. 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 the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this to execute code in the context of the current process. Was ZDI-CAN-16174.	7.8	More Details
CVE-2022-28307	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.16.02.022. 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. Crafted data in a DXF 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-16306.	7.8	More Details
CVE-2022-43618	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Corel CorelDRAW Graphics Suite 23.5.0.506. 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 PCX files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16377.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43617	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Corel CorelDRAW Graphics Suite 23.5.0.506. 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 PCX files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16372.	7.8	More Details
CVE-2022-43616	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Corel CorelDRAW Graphics Suite 23.5.0.506. 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 EMF 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 object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16371.	7.8	More Details
CVE-2023-26775	File Upload vulnerability found in Monitorr v.1.7.6 allows a remote attacker t oexecute arbitrary code via a crafted file upload to the assets/php/upload.php endpoint.	7.8	More Details
CVE-2022-43614	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Corel CorelDRAW Graphics Suite 23.5.0.506. 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 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 object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16357.	7.8	More Details
CVE-2022-43613	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Corel CorelDRAW Graphics Suite 23.5.0.506. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. When parsing CGM files, the process does not properly validate 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-16356.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26733	Buffer Overflow vulnerability found in tinyTIFF v.3.0 allows a local attacker to cause a denial of service via the TinyTiffReader_readNextFrame function in tinytiffreader.c file.	7.8	More Details
CVE-2022-43609	This vulnerability allows remote attackers to execute arbitrary code on affected installations of IronCAD. 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 STP files. When parsing the VECTOR element, the process does not properly initialize a pointer prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-17672.	7.8	More Details
CVE-2023-26269	Apache James server version 3.7.3 and earlier provides a JMX management service without authentication by default. This allows privilege escalation by a malicious local user. Administrators are advised to disable JMX, or set up a JMX password. Note that version 3.7.4 onward will set up a JMX password automatically for Guice users.	7.8	More Details
CVE-2022-28310	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.034. 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 SKP 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-16339.	7.8	More Details
CVE-2022-43649	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 12.0.2.12465. 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-19478.	7.8	More Details
CVE-2023-27760	An issue found in Wondershare Technology Co, Ltd Filmora v.12.0.9 allows a remote attacker to execute arbitrary commands via the filmora_setup_full846.exe.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42430	This vulnerability allows local attackers to escalate privileges on affected Tesla vehicles. An attacker must first obtain the ability to execute privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of the wowlan_config data structure. 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 root. Was ZDI-CAN-17543.	7.8	More Details
CVE-2023-27767	An issue found in Wondershare Technology Co.,Ltd Dr.Fone v.12.4.9 allows a remote attacker to execute arbitrary commands via the drfone_setup_full3360.exe file.	7.8	More Details
CVE-2023-1670	A flaw use after free in the Linux kernel Xircom 16-bit PCMCIA (PC-card) Ethernet driver was found.A local user could use this flaw to crash the system or potentially escalate their privileges on the system.	7.8	More Details
CVE-2023-25941	Dell PowerScale OneFS versions 8.2.x-9.5.0.x contain an elevation of privilege vulnerability. A low-privileged local attacker could potentially exploit this vulnerability, leading to Denial of service, escalation of privileges, and information disclosure. This vulnerability breaks the compliance mode guarantee.	7.8	More Details
CVE-2022-48227	An issue was discovered in Acuant AsureID Sentinel before 5.2.149. It allows elevation of privileges because it opens Notepad after the installation of AssureID, Identify x64, and Identify x86, aka CORE-7361.	7.8	More Details
CVE-2022-48222	An issue was discovered in Acuant AcuFill SDK before 10.22.02.03. During SDK installation, certutil.exe is called by the Acuant installer to install certificates. This window is not hidden, and is running with elevated privileges. A standard user can break out of this window, obtaining a full SYSTEM command prompt window. This results in complete compromise via arbitrary SYSTEM code execution (elevation of privileges).	7.8	More Details
CVE-2023-1393	A flaw was found in X.Org Server Overlay Window. A Use-After-Free may lead to local privilege escalation. If a client explicitly destroys the compositor overlay window (aka COW), the Xserver would leave a dangling pointer to that window in the CompScreen structure, which will trigger a use-after-free later.	7.8	More Details
CVE-2022-4744	A double-free flaw was found in the Linux kernel's TUN/TAP device driver functionality in how a user registers the device when the register_netdevice function fails (NETDEV_REGISTER notifier). This flaw allows a local user to crash or potentially escalate their privileges on the system.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28464	hci_conn_cleanup in net/bluetooth/hci_conn.c in the Linux kernel through 6.2.9 has a use-after-free (observed in hci_conn_hash_flush) because of calls to hci_dev_put and hci_conn_put. There is a double free that may lead to privilege escalation.	7.8	More Details
CVE-2023-27771	An issue found in Wondershare Technology Co.,Ltd Creative Centerr v.1.0.8 allows a remote attacker to execute arbitrary commands via the wondershareCC_setup_full10819.exe file.	7.8	More Details
CVE-2023-27770	An issue found in Wondershare Technology Co.,Ltd Edraw-max v.12.0.4 allows a remote attacker to execute arbitrary commands via the edraw-max_setup_full5371.exe file.	7.8	More Details
CVE-2023-27769	An issue found in Wondershare Technology Co.,Ltd PDF Reader v.1.0.1 allows a remote attacker to execute arbitrary commands via the pdfreader_setup_full13143.exe file.	7.8	More Details
CVE-2023-29059	3CX DesktopApp through 18.12.416 has embedded malicious code, as exploited in the wild in March 2023. This affects versions 18.12.407 and 18.12.416 of the 3CX DesktopApp Electron Windows application shipped in Update 7, and versions 18.11.1213, 18.12.402, 18.12.407, and 18.12.416 of the 3CX DesktopApp Electron macOS application.	7.8	More Details
CVE-2023-27768	An issue found in Wondershare Technology Co.,Ltd PDFelement v9.1.1 allows a remote attacker to execute arbitrary commands via the pdfelement-pro_setup_full5239.exe file.	7.8	More Details
CVE-2023-27766	An issue found in Wondershare Technology Co.,Ltd Anireel 1.5.4 allows a remote attacker to execute arbitrary commands via the anireel_setup_full9589.exe file.	7.8	More Details
CVE-2023-27761	An issue found in Wondershare Technology Co., Ltd UniConverter v.14.0.0 allows a remote attacker to execute arbitrary commands via the uniconverter14_64bit_setup_full14204.exe file.	7.8	More Details
CVE-2023-27765	An issue found in Wondershare Technology Co.,Ltd Recoverit v.10.6.3 allows a remote attacker to execute arbitrary commands via the recoverit_setup_full4134.exe file.	7.8	More Details
CVE-2023-27764	An issue found in Wondershare Technology Co.,Ltd Repairit v.3.5.4 allows a remote attacker to execute arbitrary commands via the repairit_setup_full5913.exe file.	7.8	More Details
CVE-2023-1579	Heap based buffer overflow in binutils-gdb/bfd/libbfd.c in bfd_getl64.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0182	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where an out-of-bounds write can lead to denial of service, information disclosure, and data tampering.	7.8	More Details
CVE-2023-28892	Malwarebytes AdwCleaner 8.4.0 runs as Administrator and performs an insecure file delete operation on C:\AdwCleaner\Logs\AdwCleaner_Debug.log in which the target location is user-controllable, allowing a non-admin user to escalate privileges to SYSTEM via a symbolic link.	7.8	More Details
CVE-2022-3787	A vulnerability was found in the device-mapper-multipath. The device-mapper-multipath allows local users to obtain root access, exploited alone or in conjunction with CVE-2022-41973. Local users that are able to write to UNIX domain sockets can bypass access controls and manipulate the multipath setup. This issue occurs because an attacker can repeat a keyword, which is mishandled when arithmetic ADD is used instead of bitwise OR. This could lead to local privilege escalation to root.	7.8	More Details
CVE-2021-41526	A vulnerability has been reported in the windows installer (MSI) built with InstallScript custom action. This vulnerability may allow privilege escalation when invoked ‘repair’ of the MSI which has an InstallScript custom action.	7.8	More Details
CVE-2017-6894	A vulnerability exists in FlexNet Manager Suite releases 2015 R2 SP3 and earlier (including FlexNet Manager Platform 9.2 and earlier) that affects the inventory gathering components and can be exploited by local users to perform certain actions with elevated privileges on the local system.	7.8	More Details
CVE-2023-0664	A flaw was found in the QEMU Guest Agent service for Windows. A local unprivileged user may be able to manipulate the QEMU Guest Agent's Windows installer via repair custom actions to elevate their privileges on the system.	7.8	More Details
CVE-2022-44370	NASM v2.16 was discovered to contain a heap buffer overflow in the component quote_for_pmake() asm/nasm.c:856	7.8	More Details
CVE-2023-27763	An issue found in Wondershare Technology Co.,Ltd MobileTrans v.4.0.2 allows a remote attacker to execute arbitrary commands via the mobiletrans_setup_full5793.exe file.	7.8	More Details
CVE-2023-27762	An issue found in Wondershare Technology Co., Ltd DemoCreator v.6.0.0 allows a remote attacker to execute arbitrary commands via the democreator_setup_full7743.exe file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42431	This vulnerability allows local attackers to escalate privileges on affected Tesla vehicles. An attacker must first obtain the ability to execute privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the bcmdhd driver. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of root. Was ZDI-CAN-17544.	7.8	More Details
CVE-2022-43641	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader 12.0.1.12430. 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 U3D 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-18894.	7.8	More Details
CVE-2022-28311	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.034. 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. Crafted data in a DXF 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-16341.	7.8	More Details
CVE-2022-37381	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader. 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 AFSpecial_KeystrokeEx method. 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-17110.	7.8	More Details
CVE-2022-37378	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Editor 11.1.1.53537. 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 optimization of JavaScript functions. 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-16867.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37377	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Editor 11.1.1.53537;. 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 JavaScript optimizations. The issue results from an improper optimization, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16733.	7.8	More Details
CVE-2022-28643	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.34. 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-16468.	7.8	More Details
CVE-2022-37374	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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 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-18068.	7.8	More Details
CVE-2022-37372	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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 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-17809.	7.8	More Details
CVE-2022-37371	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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 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-17772.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28644	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.34. 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-16469.	7.8	More Details
CVE-2022-37369	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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 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-17724.	7.8	More Details
CVE-2022-37367	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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. Crafted data in an AcroForm 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-17726.	7.8	More Details
CVE-2022-37366	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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 object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-17727.	7.8	More Details
CVE-2022-37365	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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 saveAs method. The application exposes a JavaScript interface that allows the attacker to write arbitrary files. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-17527.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37364	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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 EMF files. Crafted data in an EMF 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-17634.	7.8	More Details
CVE-2022-37363	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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 EMF files. Crafted data in an EMF 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-17673.	7.8	More Details
CVE-2022-37362	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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 files. Crafted data in a PNG 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-17660.	7.8	More Details
CVE-2022-28646	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.2.034. 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 IFC files. Crafted data in an IFC 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-16570.	7.8	More Details
CVE-2022-28314	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.34. 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 IFC files. Crafted data in an IFC 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-16332.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37359	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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. 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-17633.	7.8	More Details
CVE-2022-37358	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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 JPG files. Crafted data in a JPG 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-17632.	7.8	More Details
CVE-2022-37357	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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 ICO files. Crafted data in an ICO 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-17631.	7.8	More Details
CVE-2022-37356	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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 JPG files. Crafted data in a JPG 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-17630.	7.8	More Details
CVE-2022-37355	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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 JPG files. Crafted data in a JPG 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-17629.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37354	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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-17628.	7.8	More Details
CVE-2022-37350	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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 Collab 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-17144.	7.8	More Details
CVE-2022-37349	This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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 submitForm method. 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-17142.	7.8	More Details
CVE-2022-28647	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.2.034. 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 IFC files. Crafted data in an IFC 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-16573.	7.8	More Details
CVE-2022-28685	This vulnerability allows remote attackers to execute arbitrary code on affected installations of AVEVA Edge 2020 SP2 Patch 0(4201.2111.1802.0000). 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 APP files. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-17212.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28686	This vulnerability allows remote attackers to execute arbitrary code on affected installations of AVEVA Edge 2020 SP2 Patch 0(4201.2111.1802.0000). 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 APP files. The process loads a library from an unsecured location. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-17114.	7.8	More Details
CVE-2022-36970	This vulnerability allows remote attackers to execute arbitrary code on affected installations of AVEVA Edge 20.0 Build: 4201.2111.1802.0000 Service Pack 2. 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 processing of APP files. Crafted data in a APP file can cause the application to execute arbitrary Visual Basic scripts. The user interface fails to provide sufficient indication of the hazard. An attacker can leverage this vulnerability to execute code in the context of current process. Was ZDI-CAN-17370.	7.8	More Details
CVE-2022-2561	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OPC Labs QuickOPC 2022.1. 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 processing of XML files in Connectivity Explorer. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16596.	7.8	More Details
CVE-2022-28642	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.34. 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-16424.	7.8	More Details
CVE-2023-29323	ascii_load_sockaddr in smtpd in OpenBSD before 7.1 errata 024 and 7.2 before errata 020, and OpenSMTPD Portable before 7.0.0-portable commit f748277, can abort upon a connection from a local, scoped IPv6 address.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28318	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.34. 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 IFC files. Crafted data in an IFC 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-16379.	7.8	More Details
CVE-2022-28317	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.34. 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 IFC 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-16369.	7.8	More Details
CVE-2022-37389	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.2.53575. 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-17545.	7.8	More Details
CVE-2022-37391	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.2.53575. 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-17661.	7.8	More Details
CVE-2022-37388	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.2.53575. 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-17516.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28319	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.034. 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 3DM 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-16340.	7.8	More Details
CVE-2022-48226	An issue was discovered in Acuant AcuFill SDK before 10.22.02.03. During installation, an EXE gets executed out of C:\Windows\Temp. A standard user can create the path file ahead of time and obtain elevated code execution. Permissions need to be modified to prevent manipulation.	7.8	More Details
CVE-2022-37387	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.2.53575. 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-17552.	7.8	More Details
CVE-2022-28320	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.16.02.022. 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 3DM 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-16282.	7.8	More Details
CVE-2022-37385	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. 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-17301.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37390	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.2.53575. 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-17551.	7.8	More Details
CVE-2022-28641	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.34. 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 IFC 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-16390.	7.8	More Details
CVE-2022-28315	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.34. 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 IFC files. 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 the current process. Was ZDI-CAN-16367.	7.8	More Details
CVE-2022-37384	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. 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 delay method. 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-17327.	7.8	More Details
CVE-2022-28316	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.02.34. 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 IFC files. Crafted data in an IFC 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-16368.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28853	Mastodon is a free, open-source social network server based on ActivityPub Mastodon allows configuration of LDAP for authentication. Starting in version 2.5.0 and prior to versions 3.5.8, 4.0.4, and 4.1.2, the LDAP query made during login is insecure and the attacker can perform LDAP injection attack to leak arbitrary attributes from LDAP database. This issue is fixed in versions 3.5.8, 4.0.4, and 4.1.2.	7.7	More Details
CVE-2023-27489	Kiwi TCMS is an open source test management system for both manual and automated testing. Kiwi TCMS accepts SVG files uploaded by users which could potentially contain JavaScript code. If SVG images are viewed directly, i.e. not rendered in an HTML page, this JavaScript code could execute. This vulnerability has been fixed by configuring Kiwi TCMS to serve with the Content-Security-Policy HTTP header which blocks inline JavaScript in all modern browsers. This configuration change is provided in version 12.1 and users are advised to upgrade. Users unable to upgrade may set their Content-Security-Policy HTTP header manually.	7.6	More Details
CVE-2022-36982	This vulnerability allows remote attackers to read arbitrary files on affected installations of Ivanti Avalanche 6.3.3.101. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the AgentTaskHandler class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose stored session cookies, leading to further compromise. Was ZDI-CAN-15967.	7.5	More Details
CVE-2023-26976	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the ssid parameter in the form_fast_setting_wifi_set function.	7.5	More Details
CVE-2023-1580	Uncontrolled resource consumption in the logging feature in Devolutions Gateway 2023.1.1 and earlier allows an attacker to cause a denial of service by filling up the disk and render the system unusable.	7.5	More Details
CVE-2020-23259	An issue found in Jsish v.3.0.11 and before allows an attacker to cause a denial of service via the Jsi_Strlen function in the src/jsiChar.c file.	7.5	More Details
CVE-2023-28625	mod_auth_openidc is an authentication and authorization module for the Apache 2.x HTTP server that implements the OpenID Connect Relying Party functionality. In versions 2.0.0 through 2.4.13.1, when `OIDCStripCookies` is set and a crafted cookie supplied, a NULL pointer dereference would occur, resulting in a segmentation fault. This could be used in a Denial-of-Service attack and thus presents an availability risk. Version 2.4.13.2 contains a patch for this issue. As a workaround, avoid using `OIDCStripCookies`.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28726	Panasonic AiSEG2 versions 2.80F through 2.93A allows remote attackers to execute arbitrary OS commands.	7.5	More Details
CVE-2023-1751	The listed versions of Nexx Smart Home devices use a WebSocket server that does not validate if the bearer token in the Authorization header belongs to the device attempting to associate. This could allow any authorized user to receive alarm information and signals meant for other devices which leak a deviceId.	7.5	More Details
CVE-2022-47188	There is an arbitrary file reading vulnerability in Generex UPS CS141 below 2.06 version. An attacker, making use of the default credentials, could upload a backup file containing a symlink to /etc/shadow, allowing him to obtain the content of this path.	7.5	More Details
CVE-2023-26855	The hashing algorithm of ChurchCRM v4.5.3 utilizes a non-random salt value which allows attackers to use precomputed hash tables or dictionary attacks to crack the hashed passwords.	7.5	More Details
CVE-2023-1014	Improper Protection for Outbound Error Messages and Alert Signals vulnerability in Virames Vira-Investing allows Account Footprinting.This issue affects Vira-Investing: before 1.0.84.86.	7.5	More Details
CVE-2022-47189	Generex UPS CS141 below 2.06 version, allows an attacker toupload a firmware file containing an incorrect configuration, in order to disrupt the normal functionality of the device.	7.5	More Details
CVE-2022-46021	X-Man 1.0 has a SQL injection vulnerability, which can cause data leakage.	7.5	More Details
CVE-2022-37012	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of Unified Automation OPC UA C++ Demo Server 1.7.6-537. Authentication is not required to exploit this vulnerability. The specific flaw exists within the OpcUa_SecureListener_ProcessSessionCallRequest method. A crafted OPC UA message can force the server to incorrectly update a reference count. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-16927.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30350	Avanquest Software RAD PDF (PDFEscape Online) 3.19.2.2 is vulnerable to Information Leak / Disclosure. The PDFEscape Online tool provides users with a "white out" functionality for redacting images, text, and other graphics from a PDF document. However, this mechanism does not remove underlying text or PDF object specification information from the PDF. As a result, for example, redacted text may be copy-pasted by a PDF reader.	7.5	More Details
CVE-2022-30351	PDFZorro PDFZorro Online r20220428 using TCPDF 6.2.5, despite having workflows claiming to correctly remove redacted information from a supplied PDF file, does not properly sanitize this information in all cases, causing redacted information, including images and text embedded in the PDF file, to be leaked unintentionally. In cases where PDF text objects are present it is possible to copy-paste redacted information into the system clipboard. Once a document is "locked" and marked for redaction once, all redactions performed after this feature is triggered are vulnerable.	7.5	More Details
CVE-2023-22845	An out-of-bounds read vulnerability exists in the TGAInput::decode_pixel() functionality of OpenImageIO Project OpenImageIO v2.4.7.1. A specially crafted targa file can lead to information disclosure. An attacker can provide a malicious file to trigger this vulnerability.	7.5	More Details
CVE-2023-24472	A denial of service vulnerability exists in the FitsOutput::close() functionality of OpenImageIO Project OpenImageIO v2.4.7.1. A specially crafted ImageOutput Object can lead to denial of service. An attacker can provide malicious input to trigger this vulnerability.	7.5	More Details
CVE-2020-23258	An issue found in Jsish v.3.0.11 allows a remote attacker to cause a denial of service via the Jsi_ValueIsNumber function in ./src/jsiValue.c file.	7.5	More Details
CVE-2023-29218	The Twitter Recommendation Algorithm through ec83d01 allows attackers to cause a denial of service (reduction of reputation score) by arranging for multiple Twitter accounts to coordinate negative signals regarding a target account, such as unfollowing, muting, blocking, and reporting, as exploited in the wild in March and April 2023. NOTE: Vendor states that allowing users to unfollow, mute, block, and report tweets and accounts and the impact of these negative engagements on Twitter's ranking algorithm is a conscious design decision, rather than a security vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28840	Moby is an open source container framework developed by Docker Inc. that is distributed as Docker, Mirantis Container Runtime, and various other downstream projects/products. The Moby daemon component (`dockerd`), which is developed as moby/moby, is commonly referred to as *Docker*. Swarm Mode, which is compiled in and delivered by default in dockerd and is thus present in most major Moby downstreams, is a simple, built-in container orchestrator that is implemented through a combination of SwarmKit and supporting network code. The overlay network driver is a core feature of Swarm Mode, providing isolated virtual LANs that allow communication between containers and services across the cluster. This driver is an implementation/user of VXLAN, which encapsulates link-layer (Ethernet) frames in UDP datagrams that tag the frame with a VXLAN Network ID (VNI) that identifies the originating overlay network. In addition, the overlay network driver supports an optional, off-by-default encrypted mode, which is especially useful when VXLAN packets traverses an untrusted network between nodes. Encrypted overlay networks function by encapsulating the VXLAN datagrams through the use of the IPsec Encapsulating Security Payload protocol in Transport mode. By deploying IPSec encapsulation, encrypted overlay networks gain the additional properties of source authentication through cryptographic proof, data integrity through check-summing, and confidentiality through encryption. When setting an endpoint up on an encrypted overlay network, Moby installs three iptables (Linux kernel firewall) rules that enforce both incoming and outgoing IPSec. These rules rely on the u32 iptables extension provided by the xt_u32 kernel module to directly filter on a VXLAN packet's VNI field, so that IPSec guarantees can be enforced on encrypted overlay networks without interfering with other overlay networks or other users of VXLAN. Two iptables rules serve to filter incoming VXLAN datagrams with a VNI that corresponds to an encrypted network and discards unencrypted datagrams. The rules are appended to the end of the INPUT filter chain, following any rules that have been previously set by the system administrator. Administrator-set rules take precedence over the rules Moby sets to discard unencrypted VXLAN datagrams, which can potentially admit unencrypted datagrams that should have been discarded. The injection of arbitrary Ethernet frames can enable a Denial of Service attack. A sophisticated attacker may be able to establish a UDP or TCP connection by way of the container’s outbound gateway that would otherwise be blocked by a stateful firewall, or carry out other escalations beyond simple injection by smuggling packets into the overlay network. Patches are available in Moby releases 23.0.3 and 20.10.24. As Mirantis Container Runtime's 20.10 releases are numbered differently, users of that platform should update to 20.10.16. Some workarounds are available. Close the VXLAN port (by default, UDP port 4789) to incoming traffic at the Internet boundary to prevent all VXLAN packet injection, and/or ensure that the	7.5	More Details

CVE Number	Description	Base Score	Reference
	`xt_u32` kernel module is available on all nodes of the Swarm cluster.		
CVE-2022-4899	A vulnerability was found in zstd v1.4.10, where an attacker can supply empty string as an argument to the command line tool to cause buffer overrun.	7.5	More Details
CVE-2022-37013	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of Unified Automation OPC UA C++ Demo Server 1.7.6-537 [with vendor rollup]. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of certificates. A crafted certificate can force the server into an infinite loop. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-17203.	7.5	More Details
CVE-2023-27159	Appwrite up to v1.2.1 was discovered to contain a Server-Side Request Forgery (SSRF) via the component /v1/avatars/favicon. This vulnerability allows attackers to access network resources and sensitive information via a crafted GET request.	7.5	More Details
CVE-2023-26925	An information disclosure vulnerability exists in the Syslog functionality of D-LINK DIR-882 1.30. A specially crafted network request can lead to the disclosure of sensitive information.	7.5	More Details
CVE-2023-28877	The VTEX apps-graphql@2.x GraphQL API module does not properly restrict unauthorized access to private configuration data. (apps-graphql@3.x is unaffected by this issue.)	7.5	More Details
CVE-2020-23260	An issue found in Jsish v.3.0.11 and before allows an attacker to cause a denial of service via the StringReplaceCmd function in the src/jsiChar.c file.	7.5	More Details
CVE-2023-0836	An information leak vulnerability was discovered in HAProxy 2.1, 2.2 before 2.2.27, 2.3, 2.4 before 2.4.21, 2.5 before 2.5.11, 2.6 before 2.6.8, 2.7 before 2.7.1. There are 5 bytes left uninitialized in the connection buffer when encoding the FCGI_BEGIN_REQUEST record. Sensitive data may be disclosed to configured FastCGI backends in an unexpected way.	7.5	More Details
CVE-2023-27025	An arbitrary file download vulnerability in the background management module of RuoYi v4.7.6 and below allows attackers to download arbitrary files in the server.	7.5	More Details
CVE-2023-1656	Cleartext Transmission of Sensitive Information vulnerability in ForgeRock Inc. OpenIDM and Java Remote Connector Server (RCS) LDAP Connector on Windows, MacOS, Linux allows Remote Services with Stolen Credentials.This issue affects OpenIDM and Java Remote Connector Server (RCS): from 1.5.20.9 through 1.5.20.13.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23257	Buffer Overflow vulnerability found in Espruino 2v05.41 allows an attacker to cause a denial of service via the function jsvGarbageCollectMarkUsed in file src/jsvar.c.	7.5	More Details
CVE-2023-28509	Rocket Software UniData versions prior to 8.2.4 build 3003 and UniVerse versions prior to 11.3.5 build 1001 or 12.2.1 build 2002 use weak encryption for packet-level security and passwords transferred on the wire.	7.5	More Details
CVE-2022-36440	A reachable assertion was found in Frrouting frr-bgpd 8.3.0 in the peek_for_as4_capability function. Attackers can maliciously construct BGP open packets and send them to BGP peers running frr-bgpd, resulting in DoS.	7.5	More Details
CVE-2020-14140	When Xiaomi router firmware is updated in 2020, there is an unauthenticated API that can reveal WIFI password vulnerability. This vulnerability is caused by the lack of access control policies on some API interfaces. Attackers can exploit this vulnerability to enter the background and execute background command injection.	7.5	More Details
CVE-2019-8963	A Denial of Service (DoS) vulnerability was discovered in FlexNet Publisher's lmadmin 11.16.5, when doing a crafted POST request on lmadmin using the web-based tool.	7.5	More Details
CVE-2022-48221	An issue was discovered in Acuant AcuFill SDK before 10.22.02.03. Multiple MSI's get executed out of a standard-user writable directory. Through a race condition and OpLock manipulation, these files can be overwritten by a standard user. They then get executed by the elevated installer. This gives a standard user full SYSTEM code execution (elevation of privileges).	7.5	More Details
CVE-2023-28680	Jenkins Crap4J Plugin 0.9 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	7.5	More Details
CVE-2023-1737	A vulnerability, which was classified as critical, was found in SourceCodester Young Entrepreneur E-Negosyo System 1.0. This affects an unknown part of the file login.php. The manipulation of the argument U_USERNAME leads to sql injection. It is possible to initiate the attack remotely. The identifier VDB-224625 was assigned to this vulnerability.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1734	A vulnerability classified as critical has been found in SourceCodester Young Entrepreneur E-Negosyo System 1.0. Affected is an unknown function of the file admin/products/controller.php?action=add. The manipulation of the argument image leads to unrestricted upload. It is possible to launch the attack remotely. VDB-224622 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2023-1776	Boards in Mattermost allows an attacker to upload a malicious SVG image file as an attachment to a card and share it using a direct link to the file.	7.3	More Details
CVE-2022-48225	An issue was discovered in Acuant AcuFill SDK before 10.22.02.03. It is used to install drivers from several different vendors. The Gemalto Document Reader child installation process is vulnerable to DLL hijacking, because it attempts to execute (with elevated privileges) multiple non-existent DLLs out of a non-existent standard-user writable location.	7.3	More Details
CVE-2023-1800	A vulnerability, which was classified as critical, has been found in sjqzhang go-fastdfs up to 1.4.3. Affected by this issue is the function upload of the file /group1/uploa of the component File Upload Handler. The manipulation leads to path traversal: '../filedir'. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224768.	7.3	More Details
CVE-2022-48224	An issue was discovered in Acuant AcuFill SDK before 10.22.02.03. It is installed with insecure permissions (full write access within Program Files). Standard users can replace files within this directory that get executed with elevated privileges, leading to a complete arbitrary code execution (elevation of privileges).	7.3	More Details
CVE-2023-28733	AnyMailing Joomla Plugin is vulnerable to stored cross site scripting (XSS) in templates and emails of AcyMailing, exploitable without authentication when access is granted to the campaign's creation on front-office. This issue affects AnyMailing Joomla Plugin Enterprise in versions below 8.3.0.	7.2	More Details
CVE-2023-27160	forem up to v2022.11.11 was discovered to contain a Server-Side Request Forgery (SSRF) via the component /articles/{id}. This vulnerability allows attackers to access network resources and sensitive information via a crafted POST request.	7.2	More Details
CVE-2023-1124	The Shopping Cart & eCommerce Store WordPress plugin before 5.4.3 does not validate HTTP requests, allowing authenticated users with admin privileges to perform LFI attacks.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26830	An unrestricted file upload vulnerability in the administrative portal branding component of Gladinet CentreStack before 13.5.9808 allows authenticated attackers to execute arbitrary code by uploading malicious files to the server.	7.2	More Details
CVE-2023-27091	An unauthorized access issue found in XiaoBingby TeaCMS 2.3.3 allows attackers to escalate privileges via the id and keywords parameter(s).	7.2	More Details
CVE-2021-3267	File Upload vulnerability found in KiteCMS v.1.1 allows a remote attacker to execute arbitrary code via the uploadFile function.	7.2	More Details
CVE-2022-4934	A post-auth command injection vulnerability in the exception wizard of Sophos Web Appliance older than version 4.3.10.4 allows administrators to execute arbitrary code.	7.2	More Details
CVE-2022-36969	This vulnerability allows remote attackers to disclose sensitive information on affected installations of AVEVA Edge 2020 SP2 Patch 0(4201.2111.1802.0000). 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 LoadImportedLibraries method. Due to the improper restriction of XML External Entity (XXE) references, a crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose information in the context of the current process. Was ZDI-CAN-17394.	7.1	More Details
CVE-2022-43650	This vulnerability allows remote attackers to disclose sensitive information on affected installations of RARLAB WinRAR 6.11.0.0. 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 ZIP files. Crafted data in a ZIP 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-19232.	7.1	More Details
CVE-2023-25303	ATLauncher <= 3.4.26.0 is vulnerable to Directory Traversal. A mrpack file can be maliciously crafted to create arbitrary files outside of the installation directory.	7.1	More Details
CVE-2023-25305	PolyMC Launcher <= 1.4.3 is vulnerable to Directory Traversal. A mrpack file can be maliciously crafted to create arbitrary files outside of the installation directory.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47603	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in wpdevart Gallery – Image and Video Gallery with Thumbnails plugin <= 2.0.1 versions.	7.1	More Details
CVE-2023-1750	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could retrieve device history, set device settings, and retrieve device information.	7.1	More Details
CVE-2023-0180	NVIDIA GPU Display Driver for Linux contains a vulnerability in a kernel mode layer handler, which may lead to denial of service or information disclosure.	7.1	More Details
CVE-2023-0181	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in a kernel mode layer handler, where memory permissions are not correctly checked, which may lead to denial of service and data tampering.	7.1	More Details
CVE-2023-0191	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds access may lead to denial of service or data tampering.	7.1	More Details
CVE-2022-43941	Hitachi Vantara Pentaho Business Analytics Server versions before 9.4.0.1 and 9.3.0.2, including 8.3.x do not correctly protect the Post Analysis service endpoint of the data access plugin against out-of-band XML External Entity Reference.	7.1	More Details
CVE-2023-0183	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an out-of-bounds write can lead to denial of service and data tampering.	7.1	More Details
CVE-2023-1652	A use-after-free flaw was found in nfsd4_ssc_setup_dul in fs/nfsd/nfs4proc.c in the NFS filesystem in the Linux Kernel. This issue could allow a local attacker to crash the system or it may lead to a kernel information leak problem.	7.1	More Details
CVE-2023-22705	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Collne Inc. Welcart e-Commerce plugin <= 2.8.10 versions.	7.1	More Details
CVE-2022-47433	Unauth. Reflected Cross-Site Scripting vulnerability in Daniel Powney Multi Rating plugin <= 5.0.5 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47444	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ProfilePress Membership Team Paid Membership Plugin, Ecommerce, Registration Form, Login Form, User Profile & Restrict Content – ProfilePress plugin <= 4.5.3 versions.	7.1	More Details
CVE-2023-28999	Nextcloud is an open-source productivity platform. In Nextcloud Desktop client 3.0.0 until 3.8.0, Nextcloud Android app 3.13.0 until 3.25.0, and Nextcloud iOS app 3.0.5 until 4.8.0, a malicious server administrator can gain full access to an end-to-end encrypted folder. They can decrypt files, recover the folder structure and add new files. This issue is fixed in Nextcloud Desktop 3.8.0, Nextcloud Android 3.25.0, and Nextcloud iOS 4.8.0. No known workarounds are available.	6.9	More Details
CVE-2022-43627	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv4Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv4Data element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16147.	6.8	More Details
	Moby) is an open source container framework developed by Docker Inc. that is distributed as Docker, Mirantis Container Runtime, and various other downstream projects/products. The Moby daemon component (`dockerd`), which is developed as moby/moby is commonly referred to as *Docker*. Swarm Mode, which is compiled in and delivered by default in `dockerd` and is thus present in most major Moby downstreams, is a simple, built-in container orchestrator that is implemented through a combination of SwarmKit and supporting network code. The `overlay` network driver is a core feature of Swarm Mode, providing isolated virtual LANs that allow communication between containers and services across the cluster. This driver is an implementation/user of VXLAN, which encapsulates link-layer (Ethernet) frames in UDP datagrams that tag the frame with the VXLAN metadata, including a VXLAN Network ID (VNI) that identifies the originating overlay network. In addition, the overlay network driver supports an optional, off-by-default encrypted mode, which is especially useful when VXLAN packets traverses an untrusted network between nodes. Encrypted overlay networks function by encapsulating the VXLAN datagrams through the use of the IPsec Encapsulating Security Payload protocol in Transport mode. By deploying IPSec encapsulation, encrypted overlay networks gain the additional properties of source authentication through cryptographic proof, data integrity through check-summing, and confidentiality through encryption. When		

CVE Number	Description	Base Score	Reference
CVE-2023-28842	setting an endpoint up on an encrypted overlay network, Moby installs three iptables (Linux kernel firewall) rules that enforce both incoming and outgoing IPSec. These rules rely on the `u32` iptables extension provided by the `xt_u32` kernel module to directly filter on a VXLAN packet's VNI field, so that IPSec guarantees can be enforced on encrypted overlay networks without interfering with other overlay networks or other users of VXLAN. The `overlay` driver dynamically and lazily defines the kernel configuration for the VXLAN network on each node as containers are attached and detached. Routes and encryption parameters are only defined for destination nodes that participate in the network. The iptables rules that prevent encrypted overlay networks from accepting unencrypted packets are not created until a peer is available with which to communicate. Encrypted overlay networks silently accept cleartext VXLAN datagrams that are tagged with the VNI of an encrypted overlay network. As a result, it is possible to inject arbitrary Ethernet frames into the encrypted overlay network by encapsulating them in VXLAN datagrams. The implications of this can be quite dire, and GHSA-vwm3-crmr-xfxw should be referenced for a deeper exploration. Patches are available in Moby releases 23.0.3, and 20.10.24. As Mirantis Container Runtime's 20.10 releases are numbered differently, users of that platform should update to 20.10.16. Some workarounds are available. In multi-node clusters, deploy a global ‘pause’ container for each encrypted overlay network, on every node. For a single-node cluster, do not use overlay networks of any sort. Bridge networks provide the same connectivity on a single node and have no multi-node features. The Swarm ingress feature is implemented using an overlay network, but can be disabled by publishing ports in `host` mode instead of `ingress` mode (allowing the use of an external load balancer), and removing the `ingress` network. If encrypted overlay networks are in exclusive use, block UDP port 4789 from traffic that has not been validated by IPSec.	6.8	More Details
CVE-2022-43628	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetIPv6FirewallSettings requests to the web management portal. When parsing subelements within the IPv6FirewallRule element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16148.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43629	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetSysEmailSettings requests to the web management portal. When parsing subelements within the SetSysEmailSettings element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16149.	6.8	More Details
CVE-2022-43619	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of ConfigFileUpload requests to the web management portal. 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 execute code in the context of root. Was ZDI-CAN-16141.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28841	Moby is an open source container framework developed by Docker Inc. that is distributed as Docker, Mirantis Container Runtime, and various other downstream projects/products. The Moby daemon component (`dockerd`), which is developed as moby/moby is commonly referred to as *Docker*. Swarm Mode, which is compiled in and delivered by default in `dockerd` and is thus present in most major Moby downstreams, is a simple, built-in container orchestrator that is implemented through a combination of SwarmKit and supporting network code. The `overlay` network driver is a core feature of Swarm Mode, providing isolated virtual LANs that allow communication between containers and services across the cluster. This driver is an implementation/user of VXLAN, which encapsulates link-layer (Ethernet) frames in UDP datagrams that tag the frame with the VXLAN metadata, including a VXLAN Network ID (VNI) that identifies the originating overlay network. In addition, the overlay network driver supports an optional, off-by-default encrypted mode, which is especially useful when VXLAN packets traverses an untrusted network between nodes. Encrypted overlay networks function by encapsulating the VXLAN datagrams through the use of the IPsec Encapsulating Security Payload protocol in Transport mode. By deploying IPSec encapsulation, encrypted overlay networks gain the additional properties of source authentication through cryptographic proof, data integrity through check-summing, and confidentiality through encryption. When setting an endpoint up on an encrypted overlay network, Moby installs three iptables (Linux kernel firewall) rules that enforce both incoming and outgoing IPSec. These rules rely on the `u32` iptables extension provided by the `xt_u32` kernel module to directly filter on a VXLAN packet's VNI field, so that IPSec guarantees can be enforced on encrypted overlay networks without interfering with other overlay networks or other users of VXLAN. An iptables rule designates outgoing VXLAN datagrams with a VNI that corresponds to an encrypted overlay network for IPsec encapsulation. Encrypted overlay networks on affected platforms silently transmit unencrypted data. As a result, `overlay` networks may appear to be functional, passing traffic as expected, but without any of the expected confidentiality or data integrity guarantees. It is possible for an attacker sitting in a trusted position on the network to read all of the application traffic that is moving across the overlay network, resulting in unexpected secrets or user data disclosure. Thus, because many database protocols, internal APIs, etc. are not protected by a second layer of encryption, a user may use Swarm encrypted overlay networks to provide confidentiality, which due to this vulnerability this is no longer guaranteed. Patches are available in Moby releases 23.0.3, and 20.10.24. As Mirantis Container Runtime's 20.10 releases are numbered differently, users of that platform should update to 20.10.16. Some workarounds are available. Close the VXLAN port (by default, UDP port 4789) to outgoing traffic at the Internet boundary in order to prevent unintentionally leaking	6.8	More Details

CVE Number	Description	Base Score	Reference
	unencrypted traffic over the Internet, and/or ensure that the `xt_u32` kernel module is available on all nodes of the Swarm cluster.		
CVE-2023-28613	An issue was discovered in Samsung Exynos Mobile Processor and Baseband Modem Processor for Exynos 1280, Exynos 2200, and Exynos Modem 5300. An integer overflow in IPv4 fragment handling can occur due to insufficient parameter validation when reassembling these fragments.	6.8	More Details
CVE-2022-43623	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetWebFilterSetting requests to the web management portal. When parsing the WebFilterURLs element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140.	6.8	More Details
CVE-2022-43633	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetSysLogSettings requests to the web management portal. When parsing the IPAddress element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16154.	6.8	More Details
CVE-2022-43626	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetIPv4FirewallSettings requests to the web management portal. When parsing subelements within the IPv4FirewallRule element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16146.	6.8	More Details
CVE-2022-43632	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43624	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv6List element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16145.	6.8	More Details
CVE-2022-43631	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151.	6.8	More Details
CVE-2022-43625	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv4Settings requests to the web management portal. When parsing the NetMask element, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16144.	6.8	More Details
CVE-2023-0185	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where sign conversion issuescasting an unsigned primitive to signed may lead to denial of service or information disclosure.	6.7	More Details
CVE-2022-48223	An issue was discovered in Acuant AcuFill SDK before 10.22.02.03. During SDK repair, certutil.exe is called by the Acuant installer to repair certificates. This call is vulnerable to DLL hijacking due to a race condition and insecure permissions on the executing directory.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25940	Dell PowerScale OneFS version 9.5.0.0 contains improper link resolution before file access vulnerability in isi_gather_info. A high privileged local attacker could potentially exploit this vulnerability, leading to system takeover and it breaks the compliance mode guarantees.	6.7	More Details
CVE-2023-0977	A heap-based overflow vulnerability in Trellix Agent (Windows and Linux) version 5.7.8 and earlier, allows a remote user to alter the page heap in the macmnsvc process memory block resulting in the service becoming unavailable.	6.7	More Details
CVE-2023-28998	The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server. Starting with version 3.0.0 and prior to version 3.6.5, a malicious server administrator can gain full access to an end-to-end encrypted folder. They can decrypt files, recover the folder structure, and add new files. Users should upgrade the Nextcloud Desktop client to 3.6.5 to receive a patch. No known workarounds are available.	6.7	More Details
CVE-2023-28997	The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server. Starting with version 3.0.0 and prior to version 3.6.5, a malicious server administrator can recover and modify the contents of end-to-end encrypted files. Users should upgrade the Nextcloud Desktop client to 3.6.5 to receive a patch. No known workarounds are available.	6.7	More Details
CVE-2023-23355	An OS command injection vulnerability has been reported to affect QNAP operating systems. If exploited, the vulnerability possibly allows remote authenticated administrators to execute commands via unspecified vectors. QES is not affected. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2346 build 20230322 and later QTS 4.5.4.2374 build 20230416 and later QuTS hero h5.0.1.2348 build 20230324 and later QuTS hero h4.5.4.2374 build 20230417 and later QuTScloud c5.0.1.2374 and later	6.6	More Details
CVE-2023-0198	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where improper restriction of operations within the bounds of a memory buffer can lead to denial of service, information disclosure, and data tampering.	6.6	More Details
CVE-2023-28672	Jenkins OctoPerf Load Testing Plugin Plugin 4.5.1 and earlier does not perform a permission check in a connection test HTTP endpoint, allowing attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1819	Out of bounds read in Accessibility in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2023-1603	Permission bypass when importing or synchronizing entries in User vault in Devolutions Server 2022.3.13 and prior versions allows users with restricted rights to bypass entry permission via id collision.	6.5	More Details
CVE-2023-1574	Information disclosure in the user creation feature of a MSSQL data source in Devolutions Remote Desktop Manager 2023.1.9 and below on Windows allows an attacker with access to the user interface to obtain sensitive information via the error message dialog that displays the password in clear text.	6.5	More Details
CVE-2023-1202	Permission bypass when importing or synchronizing entries in User vault in Devolutions Remote Desktop Manager 2023.1.9 and prior versions allows users with restricted rights to bypass entry permission via id collision.	6.5	More Details
CVE-2022-43635	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of TP-Link TL-WR940N 6_211111 3.20.1(US) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the httpd service, which listens on TCP port 80 by default. The issue results from the incorrect implementation of the authentication algorithm. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-17332.	6.5	More Details
CVE-2023-0620	HashiCorp Vault and Vault Enterprise versions 0.8.0 through 1.13.1 are vulnerable to an SQL injection attack when configuring the Microsoft SQL (MSSQL) Database Storage Backend. When configuring the MSSQL plugin through the local, certain parameters are not sanitized when passed to the user-provided MSSQL database. An attacker may modify these parameters to execute a malicious SQL command. This issue is fixed in versions 1.13.1, 1.12.5, and 1.11.9.	6.5	More Details
CVE-2022-47602	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in JoomUnited WP Table Manager plugin <= 3.5.2 versions.	6.5	More Details
CVE-2023-28684	Jenkins remote-jobs-view-plugin Plugin 0.0.3 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0665	HashiCorp Vault's PKI mount issuer endpoints did not correctly authorize access to remove an issuer or modify issuer metadata, potentially resulting in denial of service of the PKI mount. This bug did not affect public or private key material, trust chains or certificate issuance. Fixed in Vault 1.13.1, 1.12.5, and 1.11.9.	6.5	More Details
CVE-2023-1817	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 112.0.5615.49 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2023-1816	Incorrect security UI in Picture In Picture in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially perform navigation spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2023-1814	Insufficient validation of untrusted input in Safe Browsing in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to bypass download checking via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2023-1821	Inappropriate implementation in WebShare in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2023-27167	Suprema BioStar 2 v2.8.16 was discovered to contain a SQL injection vulnerability via the values parameter at /users/absence?search_month=1.	6.5	More Details
CVE-2023-23681	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Labib Ahmed Image Hover Effects For WPBakery Page Builder plugin <= 4.0 versions.	6.5	More Details
CVE-2023-1330	The Redirection WordPress plugin before 1.1.4 does not add nonce verification in place when adding the redirect, which could allow attackers to add redirects via a CSRF attack.	6.5	More Details
CVE-2022-38072	An improper array index validation vulnerability exists in the stl_fix_normal_directions functionality of ADMesh Master Commit 767a105 and v0.98.4. A specially-crafted stl file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	6.5	More Details
CVE-2020-19850	An issue found in Directus API v.2.2.0 allows a remote attacker to cause a denial of service via a great amount of HTTP requests.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43771	Hitachi Vantara Pentaho Business Analytics Server versions before 9.4.0.0 and 9.3.0.1, including 8.3.x, using the Pentaho Data Access plugin exposes a service endpoint for CSV import which allows a user supplied path to access resources that are out of bounds.	6.5	More Details
CVE-2023-1822	Incorrect security UI in Navigation in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2023-1663	Coverity versions prior to 2023.3.2 are vulnerable to forced browsing, which exposes authenticated resources to unauthorized actors. The root cause of this vulnerability is an insecurely configured servlet mapping for the underlying Apache Tomcat server. As a result, the downloads directory and its contents are accessible. 5.9 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L/E:P/RL:O/RC:C)	6.5	More Details
CVE-2023-0614	The fix in 4.6.16, 4.7.9, 4.8.4 and 4.9.7 for CVE-2018-10919 Confidential attribute disclosure vi LDAP filters was insufficient and an attacker may be able to obtain confidential BitLocker recovery keys from a Samba AD DC.	6.5	More Details
CVE-2023-28158	Privilege escalation via stored XSS using the file upload service to upload malicious content. The issue can be exploited only by authenticated users which can create directory name to inject some XSS content and gain some privileges such admin user.	6.5	More Details
CVE-2023-1823	Inappropriate implementation in FedCM in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2020-36692	A reflected XSS via POST vulnerability in report scheduler of Sophos Web Appliance versions older than 4.3.10.4 allows execution of JavaScript code in the victim browser via a malicious form that must be manually submitted by the victim while logged in to SWA.	6.5	More Details
CVE-2023-25942	Dell PowerScale OneFS versions 8.2.x-9.4.x contain an uncontrolled resource consumption vulnerability. A malicious network user with low privileges could potentially exploit this vulnerability in SMB, leading to a potential denial of service.	6.5	More Details
CVE-2023-23685	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in RadiusTheme Portfolio – WordPress Portfolio plugin <= 2.8.10 versions.	6.5	More Details
CVE-2023-23686	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Brett Shumaker Simple Staff List plugin <= 2.2.2 versions.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23977	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Team Heateor WordPress Social Comments Plugin for Vkontakte Comments and Disqus Comments plugin <= 1.6.1 versions.	6.5	More Details
CVE-2023-1813	Inappropriate implementation in Extensions in Google Chrome prior to 112.0.5615.49 allowed an attacker who convinced a user to install a malicious extension to bypass file access restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2023-23670	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Team Heateor Fancy Comments WordPress plugin <= 1.2.10 versions.	6.5	More Details
CVE-2023-1749	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could send API requests that the affected devices would execute.	6.5	More Details
CVE-2023-29139	An issue was discovered in the CheckUser extension for MediaWiki through 1.39.3. When a user with checkuserlog permissions makes many CheckUserLog API requests in some configurations, denial of service can occur (RequestTimeoutException or upstream request timeout).	6.5	More Details
CVE-2023-28732	Missing access control in AnyMailing Joomla Plugin allows to list and access files containing sensitive information from the plugin itself and access to system files via path traversal, when being granted access to the campaign's creation on front-office. This issue affects AnyMailing Joomla Plugin in versions below 8.3.0.	6.5	More Details
CVE-2023-1777	Mattermost allows an attacker to request a preview of an existing message when creating a new message via the createPost API call, disclosing the contents of the linked message.	6.5	More Details
CVE-2023-27163	request-baskets up to v1.2.1 was discovered to contain a Server-Side Request Forgery (SSRF) via the component /api/baskets/{name}. This vulnerability allows attackers to access network resources and sensitive information via a crafted API request.	6.5	More Details
CVE-2023-25040	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Vova Anokhin WordPress Shortcodes Plugin — Shortcodes Ultimate plugin <= 5.12.6 versions.	6.5	More Details
CVE-2023-0343	Akuvox E11 contains a function that encrypts messages which are then forwarded. The IV vector and the key are static, and this may allow an attacker to decrypt messages.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27496	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, the OAuth filter assumes that a `state` query param is present on any response that looks like an OAuth redirect response. Sending it a request with the URI path equivalent to the redirect path, without the `state` parameter, will lead to abnormal termination of Envoy process. Versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9 contain a patch. The issue can also be mitigated by locking down OAuth traffic, disabling the filter, or by filtering traffic before it reaches the OAuth filter (e.g. via a lua script).	6.5	More Details
CVE-2022-3093	This vulnerability allows physical attackers to execute arbitrary code on affected Tesla vehicles. Authentication is not required to exploit this vulnerability. The specific flaw exists within the ice_updater update mechanism. The issue results from the lack of proper validation of user-supplied firmware. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-17463.	6.4	More Details
CVE-2023-28836	Wagtail is an open source content management system built on Django. Starting in version 1.5 and prior to versions 4.1.4 and 4.2.2, a stored cross-site scripting (XSS) vulnerability exists on ModelAdmin views within the Wagtail admin interface. A user with a limited-permission editor account for the Wagtail admin could potentially craft pages and documents that, when viewed by a user with higher privileges, could perform actions with that user's credentials. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin, and only affects sites with ModelAdmin enabled. For page, the vulnerability is in the "Choose a parent page" ModelAdmin view (`ChooseParentView`), available when managing pages via ModelAdmin. For documents, the vulnerability is in the ModelAdmin Inspect view (`InspectView`) when displaying document fields. Patched versions have been released as Wagtail 4.1.4 and Wagtail 4.2.2. Site owners who are unable to upgrade to the new versions can disable or override the corresponding functionality.	6.4	More Details
CVE-2023-1827	A vulnerability has been found in SourceCodester Centralized Covid Vaccination Records System 1.0 and classified as critical. This vulnerability affects unknown code of the file /vaccinated/admin/maintenance/manage_location.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-224842 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1793	A vulnerability was found in SourceCodester Police Crime Record Management System 1.0. It has been classified as critical. This affects an unknown part of the file /officer/assigncase.php of the component GET Parameter Handler. The manipulation of the argument caseid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-224745 was assigned to this vulnerability.	6.3	More Details
CVE-2023-1735	A vulnerability classified as critical was found in SourceCodester Young Entrepreneur E-Negosyo System 1.0. Affected by this vulnerability is an unknown functionality of the file passwordrecover.php. The manipulation of the argument phonenumber leads to sql injection. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-224623.	6.3	More Details
CVE-2023-1792	A vulnerability was found in SourceCodester Simple Mobile Comparison Website 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/fields/manage_field.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224744.	6.3	More Details
CVE-2023-1791	A vulnerability has been found in SourceCodester Simple Task Allocation System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file manage_user.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224743.	6.3	More Details
CVE-2023-1797	A vulnerability classified as critical was found in OTCMS 6.0.1. Affected by this vulnerability is an unknown functionality of the file sysCheckFile.php?mudi=sql. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-224749 was assigned to this vulnerability.	6.3	More Details
CVE-2023-1738	A vulnerability has been found in SourceCodester Young Entrepreneur E-Negosyo System 1.0 and classified as critical. This vulnerability affects unknown code of the file index.php?q=product. The manipulation of the argument search leads to sql injection. The attack can be initiated remotely. VDB-224626 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1739	A vulnerability was found in SourceCodester Simple and Beautiful Shopping Cart System 1.0 and classified as critical. This issue affects some unknown processing of the file upload.php. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224627.	6.3	More Details
CVE-2023-1826	A vulnerability, which was classified as critical, was found in SourceCodester Online Computer and Laptop Store 1.0. This affects an unknown part of the file php-ocls\admin\system_info\index.php. The manipulation of the argument img leads to unrestricted upload. It is possible to initiate the attack remotely. The identifier VDB-224841 was assigned to this vulnerability.	6.3	More Details
CVE-2022-3960	Hitachi Vantara Pentaho Business Analytics Server prior to versions 9.4.0.1 and 9.3.0.2, including 8.3.x cannot allow a system administrator to disable scripting capabilities of the Community Dashboard Editor (CDE) plugin.	6.3	More Details
CVE-2023-1785	A vulnerability was found in SourceCodester Earnings and Expense Tracker App 1.0. It has been classified as critical. Affected is an unknown function of the file manage_user.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-224700.	6.3	More Details
CVE-2023-1744	A vulnerability classified as critical was found in IBOS 4.5.5. This vulnerability affects unknown code of the component htaccess Handler. The manipulation leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224632.	6.3	More Details
CVE-2023-1773	A vulnerability was found in Rockoa 2.3.2. It has been declared as critical. This vulnerability affects unknown code of the file webmainConfig.php of the component Configuration File Handler. The manipulation leads to code injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-224674 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-1770	A vulnerability has been found in SourceCodester Grade Point Average GPA Calculator 1.0 and classified as critical. Affected by this vulnerability is the function get_scale of the file Master.php. The manipulation of the argument perc leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224671.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1611	A use-after-free flaw was found in btrfs_search_slot in fs/btrfs/ctree.c in btrfs in the Linux Kernel.This flaw allows an attacker to crash the system and possibly cause a kernel information lea	6.3	More Details
CVE-2023-1742	A vulnerability was found in IBOS 4.5.5. It has been rated as critical. Affected by this issue is some unknown functionality of the file /?r=report/api/getlist of the component Report Search. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-224630 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-1685	A vulnerability was found in HadSky up to 7.11.8. It has been declared as critical. This vulnerability affects unknown code of the file /install/index.php of the component Installation Interface. The manipulation leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-224242 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-1747	A vulnerability has been found in IBOS up to 4.5.4 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /?r=email/api/mark&op=delFromSend. The manipulation of the argument emailids leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.5.5 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-224635.	6.3	More Details
CVE-2023-1761	Cross-site Scripting in GitHub repository thorsten/phpmyfaq prior to 3.1.12.	6.3	More Details
CVE-2023-1060	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in YKM YKM CRM allows Reflected XSS.This issue affects YKM CRM: before 23.03.30.	6.1	More Details
CVE-2020-19698	Cross Site Scripting vulnerability found in Pandao Editor.md v.1.5.0 allows a remote attacker to execute arbitrary code via a crafted script to the editor parameter.	6.1	More Details
CVE-2023-0357	Helpy version 2.8.0 allows an unauthenticated remote attacker to exploit an XSS stored in the application. This is possible because the application does not correctly validate the attachments sent by customers in the ticket.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28850	Pimcore Perspective Editor provides an editor for Pimcore that allows users to add/remove/edit custom views and perspectives. This vulnerability has the potential to steal a user's cookie and gain unauthorized access to that user's account through the stolen cookie or redirect users to other malicious sites. Version 1.5.1 has a patch. As a workaround, one may apply the patch manually.	6.1	More Details
CVE-2020-19697	Cross Site Scripting vulnerability found in Pandao Editor.md v.1.5.0 allows a remote attacker to execute arbitrary code via a crafted script in the <iframe>src parameter.	6.1	More Details
CVE-2020-19699	Cross Site Scripting vulnerability found in KOHGYLW Kiftd v.1.0.18 allows a remote attacker to execute arbitrary code via the <ifram> tag in the upload file page.	6.1	More Details
CVE-2020-23327	Cross Site Scripting vulnerability found in ZblogCN ZblogPHP v.1.0 allows a local attacker to execute arbitrary code via a crafted payload in title parameter of the module management model.	6.1	More Details
CVE-2022-48433	In JetBrains IntelliJ IDEA before 2023.1 the NTLM hash could leak through an API method used in the IntelliJ IDEA built-in web server.	6.1	More Details
CVE-2023-26292	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Forcepoint Cloud Security Gateway (CSG) Portal on Web Cloud Security Gateway, Email Security Cloud (login_submit.mhtml modules), Forcepoint Web Security Portal on Hybrid (login_submit.mhtml modules) allows Reflected XSS.This issue affects Cloud Security Gateway (CSG): before 03/29/2023; Web Security: before 03/29/2023.	6.1	More Details
CVE-2023-26692	ZCBS Zijper Collectie Beheer Systeem (ZCBS), Zijper Publication Management System (ZPBS), and Zijper Image Bank Management System (ZBBS) 4.14k is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2023-26776	Cross Site Scripting vulnerability found in Monitorr v.1.7.6 allows a remote attacker to execute arbitrary code via the title parameter of the post_receiver-services.php file.	6.1	More Details
CVE-2023-1377	The Solidres WordPress plugin through 0.9.4 does not sanitise and escape numerous parameter before outputting them back in pages, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26291	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Forcepoint Cloud Security Gateway (CSG) Portal on Web Cloud Security Gateway, Email Security Cloud (login_form.mhtml modules), Forcepoint Web Security Portal on Hybrid (login_form.mhtml modules) allows Reflected XSS.This issue affects Cloud Security Gateway (CSG): before 03/29/2023; Web Security: before 03/29/2023.	6.1	More Details
CVE-2023-1013	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Virames Vira-Investing allows Cross-Site Scripting (XSS).This issue affects Vira-Investing: before 1.0.84.86.	6.1	More Details
CVE-2023-1766	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Akbim Computer Panon allows Reflected XSS.This issue affects Panon: before 1.0.2.	6.1	More Details
CVE-2022-27665	Reflected XSS (via AngularJS sandbox escape expressions) exists in Progress Ipswitch WS_FTP Server 8.6.0. This can lead to execution of malicious code and commands on the client due to improper handling of user-provided input. By inputting malicious payloads in the subdirectory searchbar or Add folder filename boxes, it is possible to execute client-side commands. For example, there is Client-Side Template Injection via subFolderPath to the ThinClient/WtmApiService.asmx/GetFileSubTree URI.	6.1	More Details
CVE-2023-0186	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where an out-of-bounds write can lead to denial of service and data tampering.	6.1	More Details
CVE-2023-0187	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds read can lead to denial of service.	6.1	More Details
CVE-2023-0738	OrangeScrum version 2.0.11 allows an external attacker to obtain arbitrary user accounts from the application. This is possible because the application returns malicious user input in the response with the content-type set to text/html.	6.1	More Details
CVE-2023-0325	Uvdesk version 1.1.1 allows an unauthenticated remote attacker to exploit a stored XSS in the application. This is possible because the application does not correctly validate the message sent by the clients in the ticket.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26290	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Forcepoint Cloud Security Gateway (CSG) Portal on Web Cloud Security Gateway, Email Security Cloud (login_reset_request.mhtml modules), Forcepoint Web Security Portal on Hybrid (login_reset_request.mhtml modules) allows Reflected XSS.This issue affects Cloud Security Gateway (CSG): before 03/29/2023; Web Security: before 03/29/2023.	6.1	More Details
CVE-2023-0486	VitalPBX version 3.2.3-8 allows an unauthenticated external attacker to obtain the instance's administrator account via a malicious link. This is possible because the application is vulnerable to XSS.	6.1	More Details
CVE-2023-28642	runc is a CLI tool for spawning and running containers according to the OCI specification. It was found that AppArmor can be bypassed when `/proc` inside the container is symlinked with a specific mount configuration. This issue has been fixed in runc version 1.1.5, by prohibiting symlinked `/proc`. See PR #3785 for details. users are advised to upgrade. Users unable to upgrade should avoid using an untrusted container image.	6.1	More Details
CVE-2022-47870	A Cross Site Scripting (XSS) vulnerability in the web SQL monitor login page in Redgate SQL Monitor 12.1.31.893 allows remote attackers to inject arbitrary web Script or HTML via the returnUrl parameter.	6.1	More Details
CVE-2020-20521	Cross Site Scripting vulnerability found in KiteCMS v.1.1 allows a remote attacker to execute arbitrary code via the comment parameter.	6.1	More Details
CVE-2020-20522	Cross Site Scripting vulnerability found in KiteCMS v.1.1 allows a remote attacker to execute arbitrary code via the registering user parameter.	6.1	More Details
CVE-2023-28851	Silverstripe Form Capture provides a method to capture simple silverstripe forms and an admin interface for users. Starting in version 0.2.0 and prior to versions 1.0.2, 1.1.0, 2.2.5, and 3.1.1, improper escaping when presenting stored form submissions allowed for an attacker to perform a Cross-Site Scripting attack. The vulnerability was initially patched in version 1.0.2, and version 1.1.0 includes this patch. The bug was then accidentally re-introduced during a merge error, and has been re-patched in versions 2.2.5 and 3.1.1. There are no known workarounds for this vulnerability.	6.1	More Details
CVE-2020-22533	Cross Site Scripting vulnerability found in Zentao allows a remote attacker to execute arbitrary code via the lang parameter	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26777	Cross Site Scripting vulnerability found in : louislam Uptime Kuma v.1.19.6 and before allows a remote attacker to execute arbitrary commands via the description, title, footer, and incident creation parameter of the status_page.js endpoint.	6.1	More Details
CVE-2023-26529	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in DupeOff.Com DupeOff plugin <= 1.6 versions.	5.9	More Details
CVE-2022-47596	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Jeffrey-WP Media Library Categories plugin <= 1.9.9 versions.	5.9	More Details
CVE-2022-47438	Auth. (editor+) Stored Cross-Site Scripting (XSS) vulnerability in WpDevArt Booking calendar, Appointment Booking System plugin <= 3.2.3 versions.	5.9	More Details
CVE-2023-23878	Auth. (editor+) Stored Cross-Site Scripting (XSS) vulnerability in flippercode WordPress Plugin for Google Maps – WP MAPS plugin <= 4.3.9 versions.	5.9	More Details
CVE-2023-23675	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Catchsquare WP Smart Preloader plugin <= 1.15 versions.	5.9	More Details
CVE-2023-27537	A double free vulnerability exists in libcurl <8.0.0 when sharing HSTS data between separate "handles". This sharing was introduced without considerations for do this sharing across separate threads but there was no indication of this fact in the documentation. Due to missing mutexes or thread locks, two threads sharing the same HSTS data could end up doing a double-free or use-after-free.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28846	Unpoly is a JavaScript framework for server-side web applications. There is a possible Denial of Service (DoS) vulnerability in the `unpoly-rails` gem that implements the Unpoly server protocol for Rails applications. This issues affects Rails applications that operate as an upstream of a load balancer's that uses passive health checks. The `unpoly-rails` gem echoes the request URL as an `X-Up-Location` response header. By making a request with exceedingly long URLs (paths or query string), an attacker can cause unpoly-rails to write a exceedingly large response header. If the response header is too large to be parsed by a load balancer downstream of the Rails application, it may cause the load balancer to remove the upstream from a load balancing group. This causes that application instance to become unavailable until a configured timeout is reached or until an active healthcheck succeeds. This issue has been fixed and released as version 2.7.2.2 which is available via RubyGems and GitHub. Users unable to upgrade may: Configure your load balancer to use active health checks, e.g. by periodically requesting a route with a known response that indicates healthiness; Configure your load balancer so the maximum size of response headers is at least twice the maximum size of a URL; or instead of changing your server configuration you may also configure your Rails application to delete redundant `X-Up-Location` headers set by unpoly-rails.	5.9	More Details
CVE-2023-27536	An authentication bypass vulnerability exists libcurl <8.0.0 in the connection reuse feature which can reuse previously established connections with incorrect user permissions due to a failure to check for changes in the CURLOPT_GSSAPI_DELEGATION option. This vulnerability affects krb5/kerberos/negotiate/GSSAPI transfers and could potentially result in unauthorized access to sensitive information. The safest option is to not reuse connections if the CURLOPT_GSSAPI_DELEGATION option has been changed.	5.9	More Details
CVE-2023-27535	An authentication bypass vulnerability exists in libcurl <8.0.0 in the FTP connection reuse feature that can result in wrong credentials being used during subsequent transfers. Previously created connections are kept in a connection pool for reuse if they match the current setup. However, certain FTP settings such as CURLOPT_FTP_ACCOUNT, CURLOPT_FTP_ALTERNATIVE_TO_USER, CURLOPT_FTP_SSL_CCC, and CURLOPT_USE_SSL were not included in the configuration match checks, causing them to match too easily. This could lead to libcurl using the wrong credentials when performing a transfer, potentially allowing unauthorized access to sensitive information.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23821	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Marcin Pietrzak Interactive Polish Map plugin <= 1.2 versions.	5.9	More Details
CVE-2023-0922	The Samba AD DC administration tool, when operating against a remote LDAP server, will by default send new or reset passwords over a signed-only connection.	5.9	More Details
CVE-2022-47607	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Usersnap plugin <= 4.16 versions.	5.9	More Details
CVE-2022-47610	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Mr Digital Simple Image Popup plugin <= 1.3.6 versions.	5.9	More Details
CVE-2022-47613	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in QuantumCloud AI ChatBot plugin <= 4.3.0 versions.	5.9	More Details
CVE-2023-23870	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in wpdevart Responsive Vertical Icon Menu plugin <= 1.5.8 versions.	5.9	More Details
CVE-2022-43473	A blind XML External Entity (XXE) vulnerability exists in the Add UCS Device functionality of ManageEngine OpManager 12.6.168. A specially crafted XML file can lead to SSRF. An attacker can serve a malicious XML payload to trigger this vulnerability.	5.8	More Details
CVE-2023-28645	Nextcloud richdocuments is a Nextcloud app integrating the office suit Collabora Online. In affected versions the secure view feature of the rich documents app can be bypassed by using unprotected internal API endpoint of the rich documents app. It is recommended that the Nextcloud Office app (richdocuments) is upgraded to 8.0.0-beta.1, 7.0.2 or 6.3.2. Users unable to upgrade may mitigate the issue by taking steps to restrict the ability to download documents. This includes ensuring that the `WOPI configuration` is configured to only serve documents between Nextcloud and Collabora. It is highly recommended to define the list of Collabora server IPs as the allow list within the Office admin settings of Nextcloud.	5.7	More Details
CVE-2023-28844	Nextcloud server is an open source home cloud implementation. In affected versions users that should not be able to download a file can still download an older version and use that for uncontrolled distribution. This issue has been addressed in versions 24.0.10 and 25.0.4. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28644	Nextcloud server is an open source home cloud implementation. In releases of the 25.0.x branch before 25.0.3 an inefficient fetch operation may impact server performances and/or can lead to a denial of service. This issue has been addressed and it is recommended that the Nextcloud Server is upgraded to 25.0.3. There are no known workarounds for this vulnerability.	5.7	More Details
CVE-2023-1575	The Mega Main Menu plugin for WordPress is vulnerable to Stored Cross-Site Scripting via some of its settings parameters in versions up to, and including, 2.2.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	5.5	More Details
CVE-2023-1550	Insertion of Sensitive Information into log file vulnerability in NGINX Agent. NGINX Agent version 2.0 before 2.23.3 inserts sensitive information into a log file. An authenticated attacker with local access to read agent log files may gain access to private keys. This issue is only exposed when the non-default trace level logging is enabled. Note: NGINX Agent is included with NGINX Instance Manager and used in conjunction with NGINX API Connectivity Manager, and NGINX Management Suite Security Monitoring.	5.5	More Details
CVE-2022-48430	In JetBrains IntelliJ IDEA before 2023.1 file content could be disclosed via an external stylesheet path in Markdown preview.	5.5	More Details
CVE-2023-26974	Irfanview v4.62 allows a user-mode write access violation via a crafted JPEG 2000 file starting at JPEG2000+0x0000000000001bf0.	5.5	More Details
CVE-2023-24399	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.2 versions.	5.5	More Details
CVE-2022-28645	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.02.34. 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-16470.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0197	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager, where a malicious user in a guest VM can cause a NULL-pointer dereference, which may lead to denial of service.	5.5	More Details
CVE-2022-43615	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Corel CorelDRAW Graphics Suite 23.5.0.506. 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 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-16370.	5.5	More Details
CVE-2022-37375	This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. 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 JPC files. Crafted data in a JPC 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-18069.	5.5	More Details
CVE-2023-27538	An authentication bypass vulnerability exists in libcurl prior to v8.0.0 where it reuses a previously established SSH connection despite the fact that an SSH option was modified, which should have prevented reuse. libcurl maintains a pool of previously used connections to reuse them for subsequent transfers if the configurations match. However, two SSH settings were omitted from the configuration check, allowing them to match easily, potentially leading to the reuse of an inappropriate connection.	5.5	More Details
CVE-2023-27734	An issue found in Eteran edb-debugger v.1.3.0 allows a local attacker to causea denial of service via the collect_symbols function in plugins/BinaryInfo/symbols.cpp.	5.5	More Details
CVE-2022-37379	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader 11.2.1.53537. 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 the AFSpecial_KeystrokeEx method. 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-17168.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37380	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader 11.2.1.53537. 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 ADBC objects. By performing actions in JavaScript, an attacker can trigger 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-17169.	5.5	More Details
CVE-2022-43640	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader 12.0.1.12430. 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-18629.	5.5	More Details
CVE-2022-28308	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.16.02.022. 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 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-16307.	5.5	More Details
CVE-2022-43610	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Corel CorelDRAW Graphics Suite 23.5.0.506. 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 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 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-16350.	5.5	More Details
CVE-2023-1753	Weak Password Requirements in GitHub repository thorsten/phpmyfaq prior to 3.1.12.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37382	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader 11.2.1.53537. 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 removeIcon method. 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-17383.	5.5	More Details
CVE-2022-43612	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Corel CorelDRAW Graphics Suite 23.5.0.506. 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 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-16355.	5.5	More Details
CVE-2022-37383	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader 11.2.1.53537. 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 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-17111.	5.5	More Details
CVE-2022-37386	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader 11.2.2.53575. 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 resetForm method. By performing actions in JavaScript, an attacker can trigger 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-17550.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43611	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Corel CorelDRAW Graphics Suite 23.5.0.506. 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 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-16351.	5.5	More Details
CVE-2023-1736	A vulnerability, which was classified as critical, has been found in SourceCodester Young Entrepreneur E-Negosyo System 1.0. Affected by this issue is some unknown functionality of the file cart/controller.php?action=add. The manipulation of the argument PROID leads to sql injection. The identifier of this vulnerability is VDB-224624.	5.5	More Details
CVE-2022-48228	An issue was discovered in Acuant AsureID Sentinel before 5.2.149. It uses the root of the C: drive for the i-Dentify and Sentinel Installer log files, aka CORE-7362.	5.5	More Details
CVE-2022-44368	NASM v2.16 was discovered to contain a null pointer deference in the NASM component	5.5	More Details
CVE-2022-44369	NASM 2.16 (development) is vulnerable to 476: Null Pointer Dereference via output/outaout.c.	5.5	More Details
CVE-2022-28309	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.16.02.022. 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 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-16308.	5.5	More Details
CVE-2022-28312	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.02.034. 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 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-16342.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28313	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.02.034. 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 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-16343.	5.5	More Details
CVE-2022-37351	This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. 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 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-17636.	5.5	More Details
CVE-2022-37352	This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. 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 WMF files. Crafted data in a WMF 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-17638.	5.5	More Details
CVE-2022-37353	This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. 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 EMF files. Crafted data in an EMF 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-17637.	5.5	More Details
CVE-2022-37360	This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. 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 EMF files. Crafted data in an EMF 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-17635.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28643	Nextcloud server is an open source home cloud implementation. In affected versions when a recipient receives 2 shares with the same name, while a memory cache is configured, the second share will replace the first one instead of being renamed to `{name} (2)`. It is recommended that the Nextcloud Server is upgraded to 25.0.3 or 24.0.9. Users unable to upgrade should avoid sharing 2 folders with the same name to the same user.	5.5	More Details
CVE-2022-37361	This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. 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. Crafted data in a JP2 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-17674.	5.5	More Details
CVE-2022-37368	This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. 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 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-17728.	5.5	More Details
CVE-2022-37370	This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-17725.	5.5	More Details
CVE-2022-37373	This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-17810.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0188	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an unprivileged user can cause improper restriction of operations within the bounds of a memory buffer cause an out-of-bounds read, which may lead to denial of service.	5.5	More Details
CVE-2022-1274	A flaw was found in Keycloak in the execute-actions-email endpoint. This issue allows arbitrary HTML to be injected into emails sent to Keycloak users and can be misused to perform phishing or other attacks against users.	5.4	More Details
CVE-2022-41633	Cross-Site Request Forgery (CSRF) vulnerability in PeepSo Community by PeepSo – Social Network, Membership, Registration, User Profiles plugin <= 6.0.2.0 versions.	5.4	More Details
CVE-2023-27488	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, escalation of privileges is possible when `failure_mode_allow: true` is configured for `ext_authz` filter. For affected components that are used for logging and/or visibility, requests may not be logged by the receiving service. When Envoy was configured to use ext_authz, ext_proc, tap, ratelimit filters, and grpc access log service and an http header with non-UTF-8 data was received, Envoy would generate an invalid protobuf message and send it to the configured service. The receiving service would typically generate an error when decoding the protobuf message. For ext_authz that was configured with ``failure_mode_allow: true``, the request would have been allowed in this case. For the other services, this could have resulted in other unforeseen errors such as a lack of visibility into requests. As of versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, Envoy by default sanitizes the values sent in gRPC service calls to be valid UTF-8, replacing data that is not valid UTF-8 with a `!` character. This behavioral change can be temporarily reverted by setting runtime guard `envoy.reloadable_features.service_sanitize_non_utf8_strings` to false. As a workaround, one may set `failure_mode_allow: false` for `ext_authz`.	5.4	More Details
CVE-2023-0399	The Image Over Image For WPBakery Page Builder WordPress plugin before 3.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29000	The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server. Starting with version 3.0.0 and prior to version 3.7.0, by trusting that the server will return a certificate that belongs to the keypair of the user, a malicious server could get the desktop client to encrypt files with a key known to the attacker. This issue is fixed in Nextcloud Desktop 3.7.0. No known workarounds are available.	5.4	More Details
CVE-2023-26283	IBM WebSphere Application Server 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 248416.	5.4	More Details
CVE-2023-27491	Envoy is an open source edge and service proxy designed for cloud-native applications. Compliant HTTP/1 service should reject malformed request lines. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, There is a possibility that non compliant HTTP/1 service may allow malformed requests, potentially leading to a bypass of security policies. This issue is fixed in versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9.	5.4	More Details
CVE-2023-28669	Jenkins JaCoCo Plugin 3.3.2 and earlier does not escape class and method names shown on the UI, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control input files for the 'Record JaCoCo coverage report' post-build action.	5.4	More Details
CVE-2023-23861	Cross-Site Request Forgery (CSRF) vulnerability in German Mesky GMAce plugin <= 1.5.2 versions.	5.4	More Details
CVE-2023-28670	Jenkins Pipeline Aggregator View Plugin 1.13 and earlier does not escape a variable representing the current view's URL in inline JavaScript, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by authenticated attackers with Overall/Read permission.	5.4	More Details
CVE-2020-19277	Cross Site Scripting vulnerability found in Phachon mm-wiki v.0.1.2 allows a remote attacker to execute arbitrary code via javascript code in the markdown editor.	5.4	More Details
CVE-2023-24724	A stored cross site scripting (XSS) vulnerability was discovered in the user management module of the SAS 9.4 Admin Console, due to insufficient validation and sanitization of data input into the user creation and editing form fields. The product name is SAS Web Administration interface (SASAdmin). For the product release, the reported version is 9.4_M2 and the fixed version is 9.4_M3. For the SAS release, the reported version is 9.4 TS1M2 and the fixed version is 9.4 TS1M3.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4771	Hitachi Vantara Pentaho Business Analytics Server prior to versions 9.4.0.1 and 9.3.0.2, including 8.3.x allow a malicious URL to inject content into the Pentaho User Console through session variables.	5.4	More Details
CVE-2023-28678	Jenkins Cppcheck Plugin 1.26 and earlier does not escape file names from Cppcheck report files before showing them on the Jenkins UI, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control report file contents.	5.4	More Details
CVE-2023-26982	Trudesk v1.2.6 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Add Tags parameter under the Create Ticket function.	5.4	More Details
CVE-2023-1701	Cross-site Scripting (XSS) - Reflected in GitHub repository pimcore/pimcore prior to 10.5.20.	5.4	More Details
CVE-2023-1702	Cross-site Scripting (XSS) - Generic in GitHub repository pimcore/pimcore prior to 10.5.20.	5.4	More Details
CVE-2023-28679	Jenkins Mashup Portlets Plugin 1.1.2 and earlier provides the "Generic JS Portlet" feature that lets a user populate a portlet using a custom JavaScript expression, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by authenticated attackers with Overall/Read permission.	5.4	More Details
CVE-2023-1703	Cross-site Scripting (XSS) - Generic in GitHub repository pimcore/pimcore prior to 10.5.20.	5.4	More Details
CVE-2023-1704	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.20.	5.4	More Details
CVE-2023-1755	Cross-site Scripting (XSS) - Generic in GitHub repository thorsten/phpmyfaq prior to 3.1.12.	5.4	More Details
CVE-2023-1745	A vulnerability, which was classified as problematic, has been found in KMPlayer 4.2.2.73. This issue affects some unknown processing in the library SHFOLDER.dll. The manipulation leads to uncontrolled search path. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The identifier VDB-224633 was assigned to this vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26485	cmark-gfm is GitHub's fork of cmark, a CommonMark parsing and rendering library and program in C. A polynomial time complexity issue in cmark-gfm may lead to unbounded resource exhaustion and subsequent denial of service. This CVE covers quadratic complexity issues when parsing text which leads with either large numbers of `_` characters. This issue has been addressed in version 0.29.0.gfm.10. Users are advised to upgrade. Users unable to upgrade should validate that their input comes from trusted sources. ### Impact A polynomial time complexity issue in cmark-gfm may lead to unbounded resource exhaustion and subsequent denial of service. ### Proof of concept ``` $ ~/cmark-gfm$ python3 -c 'pad = "_" * 100000; print(pad + "." + pad, end="")' | time ./build/src/cmark-gfm --to plaintext ``` Increasing the number 10000 in the above commands causes the running time to increase quadratically. ### Patches This vulnerability have been patched in 0.29.0.gfm.10. ### Note on cmark and cmark-gfm XXX: TBD [cmark-gfm](https://github.com/github/cmark-gfm) is a fork of [cmark](https://github.com/commonmark/cmark) that adds the GitHub Flavored Markdown extensions. The two codebases have diverged over time, but share a common core. These bugs affect both `cmark` and `cmark-gfm`. ### Credit We would like to thank @gravypod for reporting this vulnerability. ### References https://en.wikipedia.org/wiki/Time_complexity ### For more information If you have any questions or comments about this advisory: * Open an issue in [github/cmark-gfm](https://github.com/github/cmark-gfm)	5.3	More Details
CVE-2023-28756	A ReDoS issue was discovered in the Time component through 0.2.1 in Ruby through 3.2.1. The Time parser mishandles invalid URLs that have specific characters. It causes an increase in execution time for parsing strings to Time objects. The fixed versions are 0.1.1 and 0.2.2.	5.3	More Details
CVE-2023-24473	An information disclosure vulnerability exists in the TGAInput::read_tga2_header functionality of OpenImageIO Project OpenImageIO v2.4.7.1. A specially crafted targa file can lead to a disclosure of sensitive information. An attacker can provide a malicious file to trigger this vulnerability.	5.3	More Details
CVE-2023-28755	A ReDoS issue was discovered in the URI component through 0.12.0 in Ruby through 3.2.1. The URI parser mishandles invalid URLs that have specific characters. It causes an increase in execution time for parsing strings to URI objects. The fixed versions are 0.12.1, 0.11.1, 0.10.2 and 0.10.0.1.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26118	Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.	5.3	More Details
CVE-2023-26117	Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the $resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.	5.3	More Details
CVE-2023-26116	Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.	5.3	More Details
CVE-2023-24824	cmark-gfm is GitHub's fork of cmark, a CommonMark parsing and rendering library and program in C. A polynomial time complexity issue in cmark-gfm may lead to unbounded resource exhaustion and subsequent denial of service. This CVE covers quadratic complexity issues when parsing text which leads with either large numbers of `>` or `-` characters. This issue has been addressed in version 0.29.0.gfm.10. Users are advised to upgrade. Users unable to upgrade should validate that their input comes from trusted sources.	5.3	More Details
CVE-2023-1258	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in ABB Flow-X firmware on Flow-X embedded hardware (web service modules) allows Footprinting.This issue affects Flow-X: before 4.0.	5.3	More Details
CVE-2022-3192	Improper Input Validation vulnerability in ABB AC500 V2 PM5xx allows Client-Server Protocol Manipulation.This issue affects AC500 V2: from 2.0.0 before 2.8.6.	5.3	More Details
CVE-2023-26916	libyang from v2.0.164 to v2.1.30 was discovered to contain a NULL pointer dereference via the function lys_parse_mem at lys_parse_mem.c.	5.3	More Details
CVE-2023-29140	An issue was discovered in the GrowthExperiments extension for MediaWiki through 1.39.3. Attackers might be able to see edits for which the username has been hidden, because there is no check for rev_deleted.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1784	A vulnerability was found in jeecg-boot 3.5.0 and classified as critical. This issue affects some unknown processing of the component API Documentation. The manipulation leads to improper authentication. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224699.	5.3	More Details
CVE-2022-48432	In JetBrains IntelliJ IDEA before 2023.1 the bundled version of Chromium wasn't sandboxed.	5.2	More Details
CVE-2023-25000	HashiCorp Vault's implementation of Shamir's secret sharing used precomputed table lookups, and was vulnerable to cache-timing attacks. An attacker with access to, and the ability to observe a large number of unseal operations on the host through a side channel may reduce the search space of a brute force effort to recover the Shamir shares. Fixed in Vault 1.13.1, 1.12.5, and 1.11.9.	5.0	More Details
CVE-2023-25809	runc is a CLI tool for spawning and running containers according to the OCI specification. In affected versions it was found that rootless runc makes `/sys/fs/cgroup` writable in following conditons: 1. when runc is executed inside the user namespace, and the `config.json` does not specify the cgroup namespace to be unshared (e.g.., `(docker|podman|nerdctl) run --cgroupns=host`, with Rootless Docker/Podman/nerdctl) or 2. when runc is executed outside the user namespace, and `/sys` is mounted with `rbind, ro` (e.g., `runc spec --rootless`; this condition is very rare). A container may gain the write access to user-owned cgroup hierarchy `/sys/fs/cgroup/user.slice/...` on the host . Other users's cgroup hierarchies are not affected. Users are advised to upgrade to version 1.1.5. Users unable to upgrade may unshare the cgroup namespace (`(docker|podman|nerdctl) run --cgroupns=private)`. This is the default behavior of Docker/Podman/nerdctl on cgroup v2 hosts. or add `/sys/fs/cgroup` to `maskedPaths`.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28837	Wagtail is an open source content management system built on Django. Prior to versions 4.1.4 and 4.2.2, a memory exhaustion bug exists in Wagtail's handling of uploaded images and documents. For both images and documents, files are loaded into memory during upload for additional processing. A user with access to upload images or documents through the Wagtail admin interface could upload a file so large that it results in a crash of denial of service. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. It can only be exploited by admin users with permission to upload images or documents. Image uploads are restricted to 10MB by default, however this validation only happens on the frontend and on the backend after the vulnerable code. Patched versions have been released as Wagtail 4.1.4 and Wagtail 4.2.2). Site owners who are unable to upgrade to the new versions are encouraged to add extra protections outside of Wagtail to limit the size of uploaded files.	4.9	More Details
CVE-2023-27492	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, the Lua filter is vulnerable to denial of service. Attackers can send large request bodies for routes that have Lua filter enabled and trigger crashes. As of versions versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, Envoy no longer invokes the Lua coroutine if the filter has been reset. As a workaround for those whose Lua filter is buffering all requests/responses, mitigate by using the buffer filter to avoid triggering the local reply in the Lua filter.	4.8	More Details
CVE-2023-1760	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.12.	4.8	More Details
CVE-2023-1759	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.12.	4.8	More Details
CVE-2023-28848	user_oidc is the OIDC connect user backend for Nextcloud, an open source collaboration platform. A vulnerability in versions 1.0.0 until 1.3.0 effectively allowed an attacker to bypass the state protection as they could just copy the expected state token from the first request to their second request. Users should upgrade user_oidc to 1.3.0 to receive a patch for the issue. No known workarounds are available.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1740	A vulnerability was found in SourceCodester Air Cargo Management System 1.0. It has been classified as critical. Affected is an unknown function of the file admin/user/manage_user.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224628.	4.7	More Details
CVE-2023-0192	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer handler, where improper privilege management can lead to escalation of privileges and information disclosure.	4.7	More Details
CVE-2023-1754	Improper Neutralization of Input During Web Page Generation in GitHub repository thorsten/phpmyfaq prior to 3.1.12.	4.7	More Details
CVE-2023-1684	A vulnerability was found in HadSky 7.7.16. It has been classified as problematic. This affects an unknown part of the file upload/index.php?c=app&a=superadmin:index. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-224241 was assigned to this vulnerability.	4.7	More Details
CVE-2022-42452	HCL Launch is vulnerable to HTML injection. HTML code is stored and included without being sanitized. This can lead to further attacks such as XSS and Open Redirections.	4.6	More Details
CVE-2022-48431	In JetBrains IntelliJ IDEA before 2023.1 in some cases, Gradle and Maven projects could be imported without the “Trust Project” confirmation.	4.5	More Details
CVE-2022-42432	This vulnerability allows local attackers to disclose sensitive information on affected installations of the Linux Kernel 6.0-rc2. An attacker must first obtain the ability to execute high-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the nft_osf_eval function. 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 kernel. Was ZDI-CAN-18540.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1840	The Sp*tify Play Button for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 2.07 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2023-28646	Nextcloud android is an android app for interfacing with the nextcloud home server ecosystem. In versions from 3.7.0 and before 3.24.1 an attacker that has access to the unlocked physical device can bypass the Nextcloud Android Pin/passcode protection via a thirdparty app. This allows to see meta information like sharer, sharees and activity of files. It is recommended that the Nextcloud Android app is upgraded to 3.24.1. There are no known workarounds for this vulnerability.	4.4	More Details
CVE-2023-28647	Nextcloud iOS is an ios application used to interface with the nextcloud home cloud ecosystem. In versions prior to 4.7.0 when an attacker has physical access to an unlocked device, they may enable the integration into the iOS Files app and bypass the Nextcloud pin/password protection and gain access to a users files. It is recommended that the Nextcloud iOS app is upgraded to 4.7.0. There are no known workarounds for this vulnerability.	4.4	More Details
CVE-2023-1699	Rapid7 Nexpose versions 6.6.186 and below suffer from a forced browsing vulnerability. This vulnerability allows an attacker to manipulate URLs to forcefully browse to and access administrative pages. This vulnerability is fixed in version 6.6.187.	4.3	More Details
CVE-2023-1741	A vulnerability was found in jeecg-boot 3.5.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file SysDictMapper.java of the component Sleep Command Handler. The manipulation leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-224629 was assigned to this vulnerability.	4.3	More Details
CVE-2023-1769	A vulnerability, which was classified as problematic, was found in SourceCodester Grade Point Average GPA Calculator 1.0. Affected is an unknown function of the file index.php. The manipulation of the argument page with the input php://filter/read=convert.base64-encode/resource=grade_table leads to information disclosure. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-224670 is the identifier assigned to this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29137	An issue was discovered in the GrowthExperiments extension for MediaWiki through 1.39.3. The UserImpactHandler for GrowthExperiments inadvertently returns the timezone preference for arbitrary users, which can be used to de-anonymize users.	4.3	More Details
CVE-2022-38077	Cross-Site Request Forgery (CSRF) vulnerability in WP OnlineSupport, Essential Plugin Popup Anything – A Marketing Popup and Lead Generation Conversions plugin <= 2.2.1 versions.	4.3	More Details
CVE-2023-1683	A vulnerability was found in Xunrui CMS 4.61 and classified as problematic. Affected by this issue is some unknown functionality of the file /dayrui/Fcms/View/system_log.html. The manipulation leads to information disclosure. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224240.	4.3	More Details
CVE-2022-47191	Generex UPS CS141 below 2.06 version, could allow a remote attacker to upload a firmware file containing a file with modified permissions, allowing him to escalate privileges.	4.3	More Details
CVE-2023-1680	A vulnerability, which was classified as problematic, has been found in Xunrui CMS 4.61. This issue affects some unknown processing of the file /dayrui/My/View/main.html. The manipulation leads to information disclosure. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-224237 was assigned to this vulnerability.	4.3	More Details
CVE-2023-1775	When running in a High Availability configuration, Mattermost fails to sanitize some of the user_updated and post_deleted events broadcast to all users, leading to disclosure of sensitive information to some of the users with currently connected Websocket clients.	4.3	More Details
CVE-2023-1682	A vulnerability has been found in Xunrui CMS 4.61 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /dayrui/My/Config/Install.txt. The manipulation leads to direct request. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224239.	4.3	More Details
CVE-2023-28673	A missing permission check in Jenkins OctoPerf Load Testing Plugin Plugin 4.5.2 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28671	A cross-site request forgery (CSRF) vulnerability in Jenkins OctoPerf Load Testing Plugin Plugin 4.5.0 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	4.3	More Details
CVE-2022-4769	Hitachi Vantara Pentaho Business Analytics Server prior to versions 9.4.0.0 and 9.3.0.2, including 8.3.x display the target path on host when a file is uploaded with an invalid character in its name.	4.3	More Details
CVE-2022-4770	Hitachi Vantara Pentaho Business Analytics Server prior to versions 9.4.0.0 and 9.3.0.2, including 8.3.x display the full parametrized SQL query in an error message when an invalid character is used within a Pentaho Report (*.prpt).	4.3	More Details
CVE-2023-28675	A missing permission check in Jenkins OctoPerf Load Testing Plugin Plugin 4.5.2 and earlier allows attackers to connect to a previously configured Octoperf server using attacker-specified credentials.	4.3	More Details
CVE-2023-1790	A vulnerability, which was classified as problematic, was found in SourceCodester Simple Task Allocation System 1.0. Affected is an unknown function of the file index.php. The manipulation of the argument page leads to information disclosure. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224724.	4.3	More Details
CVE-2023-0225	A flaw was found in Samba. An incomplete access check on dnsHostName allows authenticated but otherwise unprivileged users to delete this attribute from any object in the directory.	4.3	More Details
CVE-2023-1774	When processing an email invite to a private channel on a team, Mattermost fails to validate the inviter's permission to that channel, allowing an attacker to invite themselves to a private channel.	4.2	More Details
CVE-2022-43772	Hitachi Vantara Pentaho Business Analytics Server versions before 9.4.0.0 and 9.3.0.1, including 8.3.x with the Big Data Plugin expose the username and password of clusters in clear text into system logs.	3.8	More Details
CVE-2023-23677	Reflected Cross-Site Scripting (XSS) vulnerability in GTmetrix GTmetrix for WordPress plugin <= 0.4.5 versions.	3.8	More Details
CVE-2023-1768	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3 (beta), and all versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the data in plaintext in certain configurations.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26112	All versions of the package configobj are vulnerable to Regular Expression Denial of Service (ReDoS) via the validate function, using (.+?)\((.*)\). **Note:** This is only exploitable in the case of a developer, putting the offending value in a server side configuration file.	3.7	More Details
CVE-2023-1687	A vulnerability classified as problematic has been found in SourceCodester Simple Task Allocation System 1.0. Affected is an unknown function of the file LoginRegistration.php?a=register_user. The manipulation of the argument Fullname leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-224244.	3.5	More Details
CVE-2023-1688	A vulnerability classified as problematic has been found in SourceCodester Earnings and Expense Tracker App 1.0. This affects an unknown part of the file Master.php?a=save_expense. The manipulation of the argument name leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-224307.	3.5	More Details
CVE-2023-1689	A vulnerability classified as problematic was found in SourceCodester Earnings and Expense Tracker App 1.0. This vulnerability affects unknown code of the file Master.php?a=save_earning. The manipulation of the argument name leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-224308.	3.5	More Details
CVE-2023-1686	A vulnerability was found in SourceCodester Young Entrepreneur E-Negosyo System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file bsenordering/admin/category/index.php of the component GET Parameter Handler. The manipulation of the argument view with the input <script>alert(233)</script> leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224243.	3.5	More Details
CVE-2023-28834	Nextcloud Server is an open source personal cloud server. Nextcloud Server 24.0.0 until 24.0.6 and 25.0.0 until 25.0.4, as well as Nextcloud Enterprise Server 23.0.0 until 23.0.11, 24.0.0 until 24.0.6, and 25.0.0 until 25.0.4, have an information disclosure vulnerability. A user was able to get the full data directory path of the Nextcloud server from an API endpoint. By itself this information is not problematic as it can also be guessed for most common setups, but it could speed up other unknown attacks in the future if the information is known. Nextcloud Server 24.0.6 and 25.0.4 and Nextcloud Enterprise Server 23.0.11, 24.0.6, and 25.0.4 contain patches for this issue. There are no known workarounds.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28835	Nextcloud server is an open source home cloud implementation. In affected versions the generated fallback password when creating a share was using a weak complexity random number generator, so when the sharer did not change it the password could be guessable to an attacker willing to brute force it. It is recommended that the Nextcloud Server is upgraded to 24.0.10 or 25.0.4. This issue only affects users who do not have a password policy enabled, so enabling a password policy is an effective mitigation for users unable to upgrade.	3.5	More Details
CVE-2023-1690	A vulnerability, which was classified as problematic, has been found in SourceCodester Earnings and Expense Tracker App 1.0. This issue affects some unknown processing of the file LoginRegistration.php?a=register_user. The manipulation of the argument fullname leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-224309 was assigned to this vulnerability.	3.5	More Details
CVE-2023-28845	Nextcloud talk is a video & audio conferencing app for Nextcloud. In affected versions the talk app does not properly filter access to a conversations member list. As a result an attacker could use this vulnerability to gain information about the members of a Talk conversation, even if they themselves are not members. It is recommended that the Nextcloud Talk is upgraded to 14.0.9 or 15.0.4. There are no known workarounds for this vulnerability.	3.5	More Details
CVE-2023-1743	A vulnerability classified as problematic has been found in SourceCodester Grade Point Average GPA Calculator 1.0. This affects an unknown part of the file index.php. The manipulation of the argument page leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224631.	3.5	More Details
CVE-2023-1746	A vulnerability, which was classified as problematic, was found in Dreamer CMS up to 3.5.0. Affected is an unknown function of the component File Upload Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. VDB-224634 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-1794	A vulnerability was found in SourceCodester Police Crime Record Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/casedetails.php of the component GET Parameter Handler. The manipulation of the argument id with the input "><script>alert(233)</script> leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-224746 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1772	A vulnerability was found in DataGear up to 4.5.1. It has been classified as problematic. This affects an unknown part of the component Diagram Type Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-224673 was assigned to this vulnerability.	3.5	More Details
CVE-2023-1771	A vulnerability was found in SourceCodester Grade Point Average GPA Calculator 1.0 and classified as problematic. Affected by this issue is the function get_scale of the file Master.php. The manipulation of the argument perc leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224672.	3.5	More Details
CVE-2023-1795	A vulnerability was found in SourceCodester Gadget Works Online Ordering System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/products/index.php of the component GET Parameter Handler. The manipulation of the argument view with the input <script>alert(666)</script> leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224747.	3.5	More Details
CVE-2023-1798	A vulnerability, which was classified as problematic, has been found in EyouCMS up to 1.5.4. Affected by this issue is some unknown functionality of the file login.php. The manipulation of the argument typename leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-224750 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-1799	A vulnerability, which was classified as problematic, was found in EyouCMS up to 1.5.4. This affects an unknown part of the file login.php. The manipulation of the argument tag_tag leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224751.	3.5	More Details
CVE-2023-26437	Denial of service vulnerability in PowerDNS Recursor allows authoritative servers to be marked unavailable.This issue affects Recursor: through 4.6.5, through 4.7.4 , through 4.8.3.	3.4	More Details
CVE-2022-48435	In JetBrains PhpStorm before 2023.1 source code could be logged in the local idea.log file	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37376	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Editor 11.1.1.53537. 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 arrays. By performing actions in JavaScript, an attacker can trigger 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-16599.	3.3	More Details
CVE-2022-27597	A vulnerability has been reported to affect QNAP operating systems. If exploited, the out-of-bounds read vulnerability allows remote authenticated administrators to get secret values. The vulnerability affects the following QNAP operating systems: QTS, QuTS hero, QuTScloud, QVP (QVR Pro appliances) We have already fixed the vulnerability in the following versions: QTS 5.0.1.2346 build 20230322 and later QuTS hero h5.0.1.2348 build 20230324 and later	2.7	More Details
CVE-2022-27598	A vulnerability has been reported to affect QNAP operating systems. If exploited, the out-of-bounds read vulnerability allows remote authenticated administrators to get secret values. The vulnerability affects the following QNAP operating systems: QTS, QuTS hero, QuTScloud, QVP (QVR Pro appliances) We have already fixed the vulnerability in the following versions: QTS 5.0.1.2346 build 20230322 and later QuTS hero h5.0.1.2348 build 20230324 and later	2.7	More Details
CVE-2023-28833	Nextcloud server is an open source home cloud implementation. In affected versions admins of a server were able to upload a logo or a favicon and to provided a file name which was not restricted and could overwrite files in the appdata directory. Administrators may have access to overwrite these files by other means but this method could be exploited by tricking an admin into uploading a maliciously named file. It is recommended that the Nextcloud Server is upgraded to 24.0.10 or 25.0.4. Users unable to upgrade should avoid ingesting logo files from untrusted sources.	2.4	More Details
CVE-2023-1796	A vulnerability classified as problematic has been found in SourceCodester Employee Payslip Generator 1.0. Affected is an unknown function of the file /classes/Master.php?f=save_position of the component Create News Handler. The manipulation of the argument name with the input <script>alert(document.cookie)</script> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224748.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0195	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer driver nvlddmkm.sys, where an can cause CWE-1284, which may lead to hypothetical Information leak of unimportant data such as local variable data of the driver	2.0	More Details
CVE-2023-0194	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer driver, where an invalid display configuration may lead to denial of service.	2.0	More Details
CVE-2023-29034	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-25587	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-2023-29035	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-29038	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-29039	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-29037	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-3487	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-29033	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-1598	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29042	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-29041	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-29040	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-29036	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details