SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 22 March 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-2023-28100	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. Versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4 contain a vulnerability similar to CVE-2017-5226, but using the `TIOCLINUX` ioctl command instead of `TIOCSTI`. If a Flatpak app is run on a Linux virtual console such as `/dev/tty1`, it can copy text from the virtual console and paste it into the command buffer, from which the command might be run after the Flatpak app has exited. Ordinary graphical terminal emulators like xterm, gnome-terminal and Konsole are unaffected. This vulnerability is specific to the Linux virtual consoles `/dev/tty1`, `/dev/tty2` and so on. A patch is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, don't run Flatpak on a Linux virtual console. Flatpak is primarily designed to be used in a Wayland or X11 graphical environment.	10.0	More Details
CVE-2022-43604	An out-of-bounds write vulnerability exists in the GetAttributeList attribute_count_request functionality of EIP Stack Group OpENer development commit 58ee13c. A specially crafted EtherNet/IP request can lead to an out-of-bounds write, potentially causing the server to crash or allow for remote code execution. An attacker can send a series of EtherNet/IP requests to trigger this vulnerability.	10.0	More Details
CVE-2022-43605	An out-of-bounds write vulnerability exists in the SetAttributeList attribute_count_request functionality of EIP Stack Group OpENer development commit 58ee13c. A specially crafted EtherNet/IP request can lead to an out of bounds write, potentially causing the server to crash or allow for remote code execution. An attacker can send a series of EtherNet/IP requests to trigger this vulnerability.	10.0	More Details
CVE-2023-27874	IBM Aspera Faspex 4.4.2 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote authenticated attacker could exploit this vulnerability to execute arbitrary commands. IBM X-Force ID: 249845.	9.9	More Details
CVE-2023-27586	CairoSVG is an SVG converter based on Cairo, a 2D graphics library. Prior to version 2.7.0, Cairo can send requests to external hosts when processing SVG files. A malicious actor could send a specially crafted SVG file that allows them to perform a server-side request forgery or denial of service. Version 2.7.0 disables CairoSVG's ability to access other files online by default.	9.9	More Details
CVE-2023-26805	Tenda W20E v15.11.0.6 (US_W20EV4.0br_v15.11.0.6(1068_1546_841)_CN_TDC) is vulnerable to Buffer Overflow via function formIPMacBindModify.	9.8	More Details
CVE-2023-28531	ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.	9.8	More Details
CVE-2023-1152	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Utarit Information Technologies Persolus allows SQL Injection. This issue affects Persolus: before 2.03.93.	9.8	More Details
CVE-2023-28115	Snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. Prior to version 1.4.2, Snappy is vulnerable to PHAR deserialization due to a lack of checking on the protocol before passing it into the `file_exists()` function. If an attacker can upload files of any type to the server he can pass in the phar:// protocol to unserialize the uploaded file and instantiate arbitrary PHP objects. This can lead to remote code execution especially when snappy is used with frameworks with documented POP chains like Laravel/Symfony vulnerable developer code. If a user can control the output file from the `generateFromHtml()` function, it will invoke deserialization. This vulnerability is capable of remote code execution if Snappy is used with frameworks or developer code with vulnerable POP chains. It has been fixed in version 1.4.2.	9.8	More Details
CVE-2023-28609	api/auth.go in Ansible Semaphore before 2.8.89 mishandles authentication.	9.8	More Details
CVE-2023-27757	An arbitrary file upload vulnerability in the /admin/user/uploadImg component of PerfreeBlog v3.1.1 allows attackers to execute arbitrary code via a crafted JPG file.	9.8	More Details
CVE-2023-26806	Tenda W20E v15.11.0.6(US_W20EV4.0br_v15.11.0.6(1068_1546_841 is vulnerable to Buffer Overflow via function formSetSysTime,	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28371	In Stellarium through 1.2, attackers can write to files that are typically unintended, such as ones with absolute pathnames or .. directory traversal.	9.8	More Details
CVE-2023-1537	Authentication Bypass by Capture-replay in GitHub repository answerdev/answer prior to 1.0.6.	9.8	More Details
CVE-2023-1153	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Pacsrapor allows SQL Injection, Command Line Execution through SQL Injection.This issue affects Pacsrapor: before 1.22.	9.8	More Details
CVE-2022-45637	An insecure password reset issue discovered in MEGAFEIS, BOFEI DBD+ Application for IOS & Android v1.4.4 service via insecure expiry mechanism.	9.8	More Details
CVE-2023-27569	The eo_tags package before 1.3.0 for PrestaShop allows SQL injection via an HTTP User-Agent or Referer header.	9.8	More Details
CVE-2023-27570	The eo_tags package before 1.4.19 for PrestaShop allows SQL injection via a crafted _ga cookie.	9.8	More Details
CVE-2023-26905	An issue was discovered in Alphaware - Simple E-Commerce System v1.0. There is a SQL injection that can directly issue instructions to the background database system via /alphaware/details.php?id.	9.8	More Details
CVE-2023-1256	The listed versions of AVEVA Plant SCADA and AVEVA Telemetry Server are vulnerable to an improper authorization exploit which could allow an unauthenticated user to remotely read data, cause denial of service, and tamper with alarm states.	9.8	More Details
CVE-2023-28461	Array Networks Array AG Series and vxAG (9.4.0.481 and earlier) allow remote code execution. An attacker can browse the filesystem on the SSL VPN gateway using a flags attribute in an HTTP header without authentication. The product could then be exploited through a vulnerable URL. The 2023-03-09 vendor advisory stated "a new Array AG release with the fix will be available soon."	9.8	More Details
CVE-2023-25280	OS Command injection vulnerability in D-Link DIR820LA1_FW105B03 allows attackers to escalate privileges to root via a crafted payload with the ping_addr parameter to ping.ccp.	9.8	More Details
CVE-2023-27239	Tenda AX3 V16.03.12.11 was discovered to contain a stack overflow via the shareSpeed parameter at /goform/WifiGuestSet.	9.8	More Details
CVE-2023-27240	Tenda AX3 V16.03.12.11 was discovered to contain a command injection vulnerability via the lanip parameter at /goform/AdvSetLanip.	9.8	More Details
CVE-2023-24726	Art Gallery Management System v1.0 was discovered to contain a SQL injection vulnerability via the viewid parameter on the enquiry page.	9.8	More Details
CVE-2020-27507	The Kamailio SIP before 5.5.0 server mishandles INVITE requests with duplicated fields and overlength tag, leading to a buffer overflow that crashes the server or possibly have unspecified other impact.	9.8	More Details
CVE-2023-25344	An issue was discovered in swig-templates thru 2.0.4 and swig thru 1.4.2, allows attackers to execute arbitrary code via crafted Object.prototype anonymous function.	9.8	More Details
CVE-2023-24468	Broken access control in Advanced Authentication versions prior to 6.4.1.1 and 6.3.7.2	9.8	More Details
CVE-2023-27041	School Registration and Fee System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at/bilal final/edit_user.php.	9.8	More Details
CVE-2023-1529	Out of bounds memory access in WebHID in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a malicious HID device. (Chromium security severity: High)	9.8	More Details
CVE-2023-23150	SA-WR915ND router firmware v17.35.1 was discovered to be vulnerable to code execution.	9.8	More Details
CVE-2023-24795	Command execution vulnerability was discovered in JHR-N916R router firmware version<=21.11.1.1483.	9.8	More Details
CVE-2023-26784	SQL Injection vulnerability found in Kirin Fortress Machine v.1.7-2020-0610 allows attackers to execute arbitrary code via the /admin.php?controller=admin_commonuser parameter.	9.8	More Details
CVE-2023-27250	Online Book Store Project v1.0 is vulnerable to SQL Injection via /bookstore/bookPerPub.php.	9.8	More Details
CVE-2023-27040	Simple Image Gallery v1.0 was discovered to contain a remote code execution (RCE) vulnerability via the username parameter.	9.8	More Details
CVE-2020-19947	Cross Site Scripting vulnerability found in Markdown Edit allows a remote attacker to execute arbitrary code via the edit parameter of the webpage.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28424	Soko if the code that powers packages.gentoo.org. Prior to version 1.0.2, the two package search handlers, `Search` and `SearchFeed`, implemented in `pkg/app/handler/packages/search.go`, are affected by a SQL injection via the `q` parameter. As a result, unauthenticated attackers can execute arbitrary SQL queries on `https://packages.gentoo.org/`. It was also demonstrated that primitive was enough to gain code execution in the context of the PostgreSQL container. The issue was addressed in commit `4fa6e4b619c0362728955b6ec56eab0e0cbf1e23y` of version 1.0.2 using prepared statements to interpolate user-controlled data in SQL queries.	9.1	More Details
CVE-2023-27578	Galaxy is an open-source platform for data analysis. All supported versions of Galaxy are affected prior to 22.01, 22.05, and 23.0 are affected by an insufficient permission check. Unsupported versions are likely affected as far back as the functionality of Visualizations/Pages exists. Due to this issue, an attacker can modify or delete any Galaxy Visualization or Galaxy Page given they know the encoded ID of it. Additionally, they can copy or import any Galaxy Visualization given they know the encoded ID of it. Patches are available for versions 22.01, 22.05, and 23.0. For the changes to take effect, you must restart all Galaxy server processes. There are no supported workarounds.	9.1	More Details
CVE-2022-44580	SQL Injection (SQLi) vulnerability in RichPlugins Plugin for Google Reviews plugin <= 2.2.3 versions.	9.1	More Details
CVE-2020-22647	An issue found in DepositGame v.1.0 allows an attacker to gain sensitive information via the GetBonusWithdraw and withdraw functions.	9.1	More Details
CVE-2022-37337	A command execution vulnerability exists in the access control functionality of Netgear Orbi Router RBR750 4.6.8.5. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.1	More Details
CVE-2023-0811	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program.	9.1	More Details
CVE-2023-21456	Path traversal vulnerability in Galaxy Themes Service prior to SMR Mar-2023 Release 1 allows attacker to access arbitrary file with system uid.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2023-27842	Insecure Permissions vulnerability found in Extplorer File manager eXtplorer v.2.1.15 allows a remote attacker to execute arbitrary code via the index.php compenent
CVE-2023-0630	The Slimstat Analytics WordPress plugin before 4.9.3.3 does not prevent subscribers from rendering shortcodes that concatenates attributes directly into an SQL query
CVE-2023-1304	An authenticated attacker can leverage an exposed getattr() method via a Jinja template to smuggle OS commands and perform other actions that are normally expect private methods. This issue was resolved in the Managed and SaaS deployments on February 1, 2023, and in version 23.2.1 of the Self-Managed version of InsightClo
CVE-2023-1543	Insufficient Session Expiration in GitHub repository answerdev/answer prior to 1.0.6.
CVE-2023-0940	The ProfileGrid WordPress plugin before 5.3.1 provides an AJAX endpoint for resetting a user password but does not implement proper authorization. This allows a use privileges, such as subscriber, to change the password of any account, including Administrator ones.
CVE-2023-25267	An issue was discovered in GFI Kerio Connect 9.4.1 patch 1 (fixed in 10.0.0). There is a stack-based Buffer Overflow in the webmail component's 2FASetup function vi authenticated request with a long primaryEMailAddress field to the webmail/api/jsonrpc URI.
CVE-2023-0340	The Custom Content Shortcode WordPress plugin through 4.0.2 does not validate one of its shortcode attribute, which could allow users with a contributor role and abo include arbitrary files via a traversal attack. This could also allow them to read non PHP files and retrieve their content. RCE could also be achieved if the attacker mana upload a malicious image containing PHP code, and then include it via the affected attribute, on a default WP install, authors could easily achieve that given that they h upload_file capability.
CVE-2023-28105	go-used-util has commonly used utility functions for Go. Versions prior to 0.0.34 have a ZipSlip issue when using fsutil package to unzip files. When users use `zip.Unz zip files from a malicious attacker, they may be vulnerable to path traversal. The issue has been fixed in version 0.0.34. There are no known workarounds.
CVE-2022-4313	A vulnerability was reported where through modifying the scan variables, an authenticated user in Tenable products, that has Scan Policy Configuration roles, could ma audit policy variables to execute arbitrary commands on credentialed scan targets.

CVE Number	Description
CVE-2023-1389	TP-Link Archer AX21 (AX1800) firmware versions before 1.1.4 Build 20230219 contained a command injection vulnerability in the country form of the /cgi-bin/luci;stok= endpoint on the web management interface. Specifically, the country parameter of the write operation was not sanitized before being used in a call to popen(), allowing unauthenticated attacker to inject commands, which would be run as root, with a simple POST request.
CVE-2023-0631	The Paid Memberships Pro WordPress plugin before 2.9.12 does not prevent subscribers from rendering shortcodes that concatenate attributes directly into an SQL qu
CVE-2023-27253	A command injection vulnerability in the function restore_rrddata() of Netgate pfSense v2.7.0 allows authenticated attackers to execute arbitrary commands via manipu contents of an XML file supplied to the component config.xml.
CVE-2023-28337	When uploading a firmware image to a Netgear Nighthawk Wifi6 Router (RAX30), a hidden “forceFWUpdate” parameter may be provided to force the upgrade to comp bypass certain validation checks. End users can use this to upload modified, unofficial, and potentially malicious firmware to the device.
CVE-2023-27037	Qibosoft QiboCMS v7 was discovered to contain a remote code execution (RCE) vulnerability via the Get_Title function at label_set_rs.php
CVE-2023-0875	The WP Meta SEO WordPress plugin before 4.5.3 does not properly sanitize and escape inputs into SQL queries, leading to a blind SQL Injection vulnerability that can exploited by subscriber+ users.
CVE-2023-0865	The WooCommerce Multiple Customer Addresses & Shipping WordPress plugin before 21.7 does not ensure that the address to add/update/retrieve/delete and duplica the user making the request, or is from a high privilege users, allowing any authenticated users, such as subscriber to add/update/duplicate/delete as well as retrieve ac other users.
CVE-2023-24760	An issue found in Ofcms v.1.1.4 allows a remote attacker to to escalate privileges via the respwd method in SysUserController.
CVE-2023-1462	Authorization Bypass Through User-Controlled Key vulnerability in Vadi Corporate Information Systems DigiKent allows Authentication Bypass, Authentication Abuse. T affects DigiKent: before 23.03.20.
CVE-2022-4009	In affected versions of Octopus Deploy it is possible for a user to introduce code via offline package creation
CVE-2023-27982	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project repo when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious d file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).
CVE-2023-1306	An authenticated attacker can leverage an exposed resource.db() accessor method to smuggle Python method calls via a Jinja template, which can lead to code execu issue was resolved in the Managed and SaaS deployments on February 1, 2023, and in version 23.2.1 of the Self-Managed version of InsightCloudSec.
CVE-2023-27980	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe (V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior)
CVE-2023-1530	Use after free in PDF in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium s severity: High)
CVE-2023-0100	In Eclipse BIRT, starting from version 2.6.2, the default configuration allowed to retrieve a report from the same host using an absolute HTTP path for the report parame __report=http://xyz.com/report.rptdesign). If the host indicated in the __report parameter matched the HTTP Host header value, the report would be retrieved. However header can be tampered with on some configurations where no virtual hosts are put in place (e.g. in the default configuration of Apache Tomcat) or when the default ho the BIRT server. This vulnerability was patched on Eclipse BIRT 4.13.
CVE-2023-24731	Simple Customer Relationship Management System v1.0 as discovered to contain a SQL injection vulnerability via the query parameter in the user profile update functi
CVE-2023-1534	Out of bounds read in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had compromised the renderer process to potentially exploit h corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-1533	Use after free in WebProtect in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chro security severity: High)
CVE-2023-27103	Libde265 v1.0.11 was discovered to contain a heap buffer overflow via the function derive_collocated_motion_vectors at motion.cc.

CVE Number	Description
CVE-2023-1532	Out of bounds read in GPU Video in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. security severity: High)
CVE-2023-1531	Use after free in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromiu severity: High)
CVE-2023-24732	Simple Customer Relationship Management System v1.0 as discovered to contain a SQL injection vulnerability via the gender parameter in the user profile update func
CVE-2023-1528	Use after free in Passwords in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had compromised the renderer process to potentially exploit hea via a crafted HTML page. (Chromium security severity: High)
CVE-2023-1471	The WP Popup Banners plugin for WordPress is vulnerable to SQL Injection via the 'banner_id' parameter in versions up to, and including, 1.2.5 due to insufficient esca user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with minimal permissions, such subscrber, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
CVE-2023-24728	Simple Customer Relationship Management System v1.0 as discovered to contain a SQL injection vulnerability via the contact parameter in the user profile update func
CVE-2023-24729	Simple Customer Relationship Management System v1.0 as discovered to contain a SQL injection vulnerability via the address parameter in the user profile update fun
CVE-2023-24730	Simple Customer Relationship Management System v1.0 as discovered to contain a SQL injection vulnerability via the company parameter in the user profile update fu
CVE-2022-42333	x86/HVM pinned cache attributes mis-handling T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to whi allow cachability control for HVM guests with passed through devices, an interface exists to explicitly override defaults which would otherwise be put in place. While not the affected guests themselves, the interface specifically exists for domains controlling such guests. This interface may therefore be used by not fully privileged entities, running deprivileged in Dom0 or qemu running in a so called stub-domain. With this exposure it is an issue that - the number of the such controlled regions was unbour 2022-42333), - installation and removal of such regions was not properly serialized (CVE-2022-42334).
CVE-2023-26497	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. I corruption can occur when processing Session Description Negotiation for Video Configuration Attribute.
CVE-2023-1262	Missing MAC layer security in Silicon Labs Wi-SUN Linux Border Router v1.5.2 and earlier allows malicious node to route malicious messages through network.
CVE-2023-26484	KubeVirt is a virtual machine management add-on for Kubernetes. In versions 0.59.0 and prior, if a malicious user has taken over a Kubernetes node where virt-handle KubeVirt node-daemon) is running, the virt-handler service account can be used to modify all node specs. This can be misused to lure-in system-level-privileged compo can, for instance, read all secrets on the cluster, or can exec into pods on other nodes. This way, a compromised node can be used to elevate privileges beyond the no potentially having full privileged access to the whole cluster. The simplest way to exploit this, once a user could compromise a specific node, is to set with the virt-handl account all other nodes to unschedulable and simply wait until system-critical components with high privileges appear on its node. No patches are available as of time c publication. As a workaround, gatekeeper users can add a webhook which will block the `virt-handler` service account to modify the spec of a node.
CVE-2023-1261	Missing MAC layer security in Silicon Labs Wi-SUN SDK v1.5.0 and earlier allows malicious node to route malicious messages through network.
CVE-2022-45636	An issue discovered in MEGAFEIS, BOFEI DBD+ Application for IOS & Android v1.4.4 allows attacker to unlock model(s) without authorization via arbitrary API reques
CVE-2023-0391	MGT-COMMERCE CloudPanel ships with a static SSL certificate to encrypt communications to the administrative interface, shared across every installation of CloudPa behavior was observed in version 2.2.0. There has been no indication from the vendor this has been addressed in version 2.2.1.
CVE-2022-43663	An integer conversion vulnerability exists in the SORBAx64.dll RecvPacket functionality of WellinTech KingHistorian 35.01.00.05. A specially crafted network packet ca buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.
CVE-2022-43441	A code execution vulnerability exists in the Statement Bindings functionality of Ghost Foundation node-sqlite3 5.1.1. A specially-crafted Javascript file can lead to arbitra execution. An attacker can provide malicious input to trigger this vulnerability.

CVE Number	Description
CVE-2023-28116	Contiki-NG is an open-source, cross-platform operating system for internet of things (IoT) devices. In versions 4.8 and prior, an out-of-bounds write can occur in the BL module of the Contiki-NG operating system. The network stack of Contiki-NG uses a global buffer (packetbuf) for processing of packets, with the size of PACKETBUF_ particular, when using the BLE L2CAP module with the default configuration, the PACKETBUF_SIZE value becomes larger then the actual size of the packetbuf. When packets are processed by the L2CAP module, a buffer overflow can therefore occur when copying the packet data to the packetbuf. The vulnerability has been patched "develop" branch of Contiki-NG, and will be included in release 4.9. The problem can be worked around by applying the patch manually.
CVE-2023-1305	An authenticated attacker can leverage an exposed “box” object to read and write arbitrary files from disk, provided those files can be parsed as yaml or JSON. This iss resolved in the Managed and SaaS deployments on February 1, 2023, and in version 23.2.1 of the Self-Managed version of InsightCloudSec.
CVE-2023-28108	Pimcore is an open source data and experience management platform. Prior to version 10.5.19, quoting is not done properly in UUID DAO model. There is the theoreti possibility to inject custom SQL if the developer is using this methods with input data and not doing proper input validation in advance and so relies on the auto-quoting by the DAO class. Users should update to version 10.5.19 to receive a patch or, as a workaround, apply the patch manually.
CVE-2023-0598	GE Digital Proficy iFIX 2022, GE Digital Proficy iFIX v6.1, and GE Digital Proficy iFIX v6.5 are vulnerable to code injection, which may allow an attacker to insert malicio configuration files in the expected web server execution path and gain full control of the HMI software.
CVE-2022-48423	In the Linux kernel before 6.1.3, fs/ntfs3/record.c does not validate resident attribute names. An out-of-bounds write may occur.
CVE-2023-1489	A vulnerability has been found in Lespeed WiseCleaner Wise System Monitor 1.5.3.54 and classified as critical. Affected by this vulnerability is the function 0x9C40208 library WiseHDInfo64.dll of the component IoControlCode Handler. The manipulation leads to improper access controls. The attack needs to be approached locally. Th been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223375.
CVE-2023-27981	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim open a malicious report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and p Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).
CVE-2023-24229	DrayTek Vigor2960 v1.5.1.4 allows an authenticated attacker with network access to the web management interface to inject operating system commands via the main 'parameter' parameter. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.
CVE-2023-27978	A CWE-502: Deserialization of Untrusted Data vulnerability exists in the Dashboard module that could cause an interpretation of malicious payload data, potentially lea remote code execution when an attacker gets the user to open a malicious file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), I Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).
CVE-2022-48422	ONLYOFFICE Docs through 7.3 on certain Linux distributions allows local users to gain privileges via a Trojan horse libgcc_s.so.1 in the current working directory, whic any directory in which an ONLYOFFICE document is located.
CVE-2022-48424	In the Linux kernel before 6.1.3, fs/ntfs3/inode.c does not validate the attribute name offset. An unhandled page fault may occur.
CVE-2022-42332	x86 shadow plus log-dirty mode use-after-free In environments where host assisted address translation is necessary but Hardware Assisted Paging (HAP) is unavailab run guests in so called shadow mode. Shadow mode maintains a pool of memory used for both shadow page tables as well as auxiliary data structures. To migrate or s guests, Xen additionally runs them in so called log-dirty mode. The data structures needed by the log-dirty tracking are part of aformentioned auxiliary data. In order to handling efforts within reasonable bounds, for operations which may require memory allocations shadow mode logic ensures up front that enough memory is available case requirements. Unfortunately, while page table memory is properly accounted for on the code path requiring the potential establishing of new shadows, demands b dirty infrastructure were not taken into consideration. As a result, just established shadow page tables could be freed again immediately, while other code is still access the assumption that they would remain allocated.
CVE-2022-48425	In the Linux kernel through 6.2.7, fs/ntfs3/inode.c has an invalid kfree because it does not validate MFT flags before replaying logs.
CVE-2023-28617	org-babel-execute:latex in ob-latex.el in Org Mode through 9.6.1 for GNU Emacs allows attackers to execute arbitrary commands via a file name or directory name that shell metacharacters.
CVE-2023-24671	VX Search v13.8 and v14.7 was discovered to contain an unquoted service path vulnerability which allows attackers to execute arbitrary commands at elevated privileg crafted executable file.
CVE-2023-27781	jpegoptim v1.5.2 was discovered to contain a heap overflow in the optimize function at jpegoptim.c.
CVE-2021-31637	An issue found in UwAmp v.1.1, 1.2, 1.3, 2.0, 2.1, 2.2, 2.2.1, 3.0.0, 3.0.1, 3.0.2 allows a remote attacker to execute arbitrary code via a crafted DLL.
CVE-2023-27984	A CWE-20: Improper Input Validation vulnerability exists in Custom Reports that could cause a macro to be executed, potentially leading to remote code execution whe opens a malicious report file planted by an attacker. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoar (V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).

CVE Number	Description
CVE-2023-27783	An issue found in TCPreplay tcprewrite v.4.4.3 allows a remote attacker to cause a denial of service via the tcpedit_dlt_cleanup function at plugins/dlt_plugins.c.
CVE-2023-26768	Buffer Overflow vulnerability found in Liblouis v.3.24.0 allows a remote attacker to cause a denial of service via the compileTranslationTable.c and lou_setDataPath fun
CVE-2023-26769	Buffer Overflow vulnerability found in Liblouis Lou_Trace v.3.24.0 allows a remote attacker to cause a denial of service via the resolveSubtable function at compileTranslationTabel.c.
CVE-2022-34422	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2023-27875	IBM Aspera Faspex 5.0.4 could allow a user to change other user's credentials due to improper access controls. IBM X-Force ID: 249847.
CVE-2023-26767	Buffer Overflow vulnerability found in Liblouis v.3.24.0 allows a remote attacker to cause a denial of service via the lou_logFile function at logginc.c endpoint.
CVE-2022-34423	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2022-45124	An information disclosure vulnerability exists in the User authentication functionality of WellinTech KingHistorian 35.01.00.05. A specially crafted network packet can lea disclosure of sensitive information. An attacker can sniff network traffic to leverage this vulnerability.
CVE-2023-24709	An issue found in Paradox Security Systems IPR512 allows attackers to cause a denial of service via the login.html and login.xml parameters.
CVE-2023-26513	Excessive Iteration vulnerability in Apache Software Foundation Apache Sling Resource Merger.This issue affects Apache Sling Resource Merger: from 1.2.0 before 1.
CVE-2023-27784	An issue found in TCPReplay v.4.4.3 allows a remote attacker to cause a denial of service via the read_hexstring function at the utils.c:309 endpoint.
CVE-2023-27785	An issue found in TCPreplay TCPprep v.4.4.3 allows a remote attacker to cause a denial of service via the parse endpoints function.
CVE-2023-27786	An issue found in TCPprep v.4.4.3 allows a remote attacker to cause a denial of service via the macinstring function.
CVE-2023-27787	An issue found in TCPprep v.4.4.3 allows a remote attacker to cause a denial of service via the parse_list function at the list.c:81 endpoint.
CVE-2023-27788	An issue found in TCPrewrite v.4.4.3 allows a remote attacker to cause a denial of service via the ports2PORT function at the portmap.c:69 endpoint.
CVE-2023-27789	An issue found in TCPprep v.4.4.3 allows a remote attacker to cause a denial of service via the cidr2cidr function at the cidr.c:178 endpoint.
CVE-2023-28104	`silverstripe/graphql` serves Silverstripe data as GraphQL representations. In versions 4.2.2 and 4.1.1, an attacker could use a specially crafted graphql query to execu of service attack against a website which has a publicly exposed graphql endpoint. This mostly affects websites with particularly large/complex graphql schemas. Users upgrade to `silverstripe/graphql` 4.2.3 or 4.1.2 to remedy the vulnerability.
CVE-2023-28118	kaml provides YAML support for kotlinx.serialization. Prior to version 0.53.0, applications that use kaml to parse untrusted input containing anchors and aliases may cor excessive memory and crash. Version 0.53.0 and later default to refusing to parse YAML documents containing anchors and aliases. There are no known workarounds
CVE-2022-34420	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.

CVE Number	Description
CVE-2022-43606	A use-of-uninitialized-pointer vulnerability exists in the Forward Open connection_management_entry functionality of EIP Stack Group OpENer development commit 58 specially-crafted EtherNet/IP request can lead to use of a null pointer, causing the server to crash. An attacker can send a series of EtherNet/IP requests to trigger this
CVE-2023-1390	A remote denial of service vulnerability was found in the Linux kernel's TIPC kernel module. The while loop in tipc_link_xmit() hits an unknown state while attempting to SKBs, which are not in the queue. Sending two small UDP packets to a system with a UDP bearer results in the CPU utilization for the system to instantly spike to 100 denial of service condition.
CVE-2021-46877	jackson-databind 2.10.x through 2.12.x before 2.12.6 and 2.13.x before 2.13.1 allows attackers to cause a denial of service (2 GB transient heap usage per read) in un situations involving JsonNode JDK serialization.
CVE-2023-26113	Versions of the package collection.js before 6.8.1 are vulnerable to Prototype Pollution via the extend function in Collection.js/dist/node/iterators/extend.js.
CVE-2023-24678	A vulnerability in Centralite Pearl Thermostat 0x04075010 allows attackers to cause a Denial of Service (DoS) via a crafted Zigbee message.
CVE-2023-27591	Miniflux is a feed reader. Prior to version 2.0.43, an unauthenticated user can retrieve Prometheus metrics from a publicly reachable Miniflux instance where the `METRICS_COLLECTOR` configuration option is enabled and `METRICS_ALLOWED_NETWORKS` is set to `127.0.0.1/8` (the default). A patch is available in Miniflux a workaround, set `METRICS_COLLECTOR` to `false` (default) or run Miniflux behind a trusted reverse-proxy.
CVE-2022-34421	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2022-34409	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2022-34419	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2023-1545	SQL Injection in GitHub repository nilsteampassnet/teampass prior to 3.0.0.23.
CVE-2023-28338	Any request send to a Netgear Nighthawk Wifi6 Router (RAX30)'s web service containing a "Content-Type" of "multipartboundary=" will result in the request body being "/tmp/mulipartFile" on the device itself. A sufficiently large file will cause device resources to be exhausted, resulting in the device becoming unusable until it is reboote
CVE-2023-1314	A vulnerability has been discovered in cloudflared's installer (<= 2023.3.0) for Windows 32-bits devices that allows a local attacker with no administrative permissions to their privileges on the affected device. This vulnerability exists because the MSI installer used by cloudflared relied on a world-writable directory. An attacker with local a the device (without Administrator rights) can use symbolic links to trick the MSI installer into deleting files in locations that the attacker would otherwise have no access creating a symlink from the world-writable directory to the target file, the attacker can manipulate the MSI installer's repair functionality to delete the target file during the process. Exploitation of this vulnerability could allow an attacker to delete important system files or replace them with malicious files, potentially leading to the affected compromised. The cloudflared client itself is not affected by this vulnerability, only the installer for 32-bit Windows devices.
CVE-2023-28097	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.9 and 3.2.6, a malformed SIP message containing a large _Content-Lengt a specially crafted Request-URI causes a segmentation fault in OpenSIPS. This issue occurs when a large amount of shared memory using the `-m` flag was allocated OpenSIPS, such as 10 GB of RAM. On the test system, this issue occurred when shared memory was set to `2362` or higher. This issue is fixed in versions 3.1.9 and only workaround is to guarantee that the Content-Length value of input messages is never larger than `2147483647`.
CVE-2023-28095	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Versions prior to 3.1.7 and 3.2.4 have a potential issue in `msg_translator.c:2628` which might server crash. This issue was found while fuzzing the function `build_res_buf_from_sip_req` but could not be reproduced against a running instance of OpenSIPS. This not be exploited against a running instance of OpenSIPS since no public function was found to make use of this vulnerable code. Even in the case of exploitation throu vectors, it is highly unlikely that this issue would lead to anything other than Denial of Service. This issue has been fixed in versions 3.1.7 and 3.2.4.
CVE-2023-27601	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, OpenSIPS crashes when a malformed SDP body is received a processed by the `delete_sdp_line` function in the sipmsgops module. This issue can be reproduced by calling the function with an SDP body that does not terminate b (i.e. `\n`). The vulnerability was found while performing black-box fuzzing against an OpenSIPS server running a configuration that made use of the functions `codec_delete_except_re` and `codec_delete_re`. The same issue was also discovered while performing coverage guided fuzzing on the function `codec_delete_excep crash happens because the function `delete_sdp_line` expects that an SDP line is terminated by a line feed (`\n`): By abusing this vulnerability, an attacker is able to cr server. It affects configurations containing functions that rely on the affected code, such as the function `codec_delete_except_re`. Due to the sanity check that is perfo `del_lump` function, exploitation of this issue will generate an `abort` in the lumps processing function, resulting in a Denial of Service. This issue has been fixed in vers and 3.2.4.

CVE Number	Description
CVE-2023-27600	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, OpenSIPS crashes when a malformed SDP body is received a processed by the `delete_sdp_line` function in the sipmsgops module. This issue can be reproduced by calling the function with an SDP body that does not terminate b (i.e. `\n`). The vulnerability was found while performing black-box fuzzing against an OpenSIPS server running a configuration that made use of the functions `codec_delete_except_re` and `codec_delete_re`. The same issue was also discovered while performing coverage guided fuzzing on the function `codec_delete_excep crash happens because the function `delete_sdp_line` expects that an SDP line is terminated by a line feed (`\n`). By abusing this vulnerability, an attacker is able to cr server. It affects configurations containing functions that rely on the affected code, such as the function `codec_delete_except_re`. Due to the sanity check that is perfor `del_lump` function, exploitation of this issue will generate an `abort` in the lumps processing function, resulting in a Denial of Service. This issue is patched in versions 3.2.4.
CVE-2022-34418	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2023-27599	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, when the function `append_hf` handles a SIP message with a To header, a call to the function `abort()` is performed, resulting in a crash. This is due to the following check in `data_lump.c:399` in the function `anchor_lump`. An att abusing this vulnerability will crash OpenSIPS leading to Denial of Service. It affects configurations containing functions that make use of the affected code, such as the `append_hf`. This issue has been fixed in versions 3.1.7 and 3.2.4.
CVE-2023-27598	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, sending a malformed `Via` header to OpenSIPS triggers a seg fault when the function `calc_tag_suffix` is called. A specially crafted `Via` header, which is deemed correct by the parser, will pass uninitialized strings to the function `MD5StringArray` which leads to the crash. Abuse of this vulnerability leads to Denial of Service due to a crash. Since the uninitialized string points to memory location further exploitation appears to be possible. No special network privileges are required to perform this attack, as long as the OpenSIPS configuration makes use of funct `sl_send_reply` or `sl_gen_totag` that trigger the vulnerable code. This issue has been fixed in versions 3.1.7 and 3.2.4.
CVE-2023-27597	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.8 and 3.2.5, when a specially crafted SIP message is processed by the fun `rewrite_ruri`, a crash occurs due to a segmentation fault. This issue causes the server to crash. It affects configurations containing functions that make use of the affec such as the function `setport`. This issue has been fixed in version 3.1.8 and 3.2.5.
CVE-2023-27596	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.8 and 3.2.5, OpenSIPS crashes when a malformed SDP body is sent multi an OpenSIPS configuration that makes use of the `stream_process` function. This issue was discovered during coverage guided fuzzing of the function `codec_delete_ By abusing this vulnerability, an attacker is able to crash the server. It affects configurations containing functions that rely on the affected code, such as the function `codec_delete_except_re`. This issue has been fixed in version 3.1.8 and 3.2.5.
CVE-2023-25345	Directory traversal vulnerability in swig-templates thru 2.0.4 and swig thru 1.4.2, allows attackers to read arbitrary files via the include or extends tags.
CVE-2023-27871	IBM Aspera Faspex 4.4.2 could allow a remote attacker to obtain sensitive credential information for an external user, using a specially crafted SQL query. IBM X-Force 249613.
CVE-2022-45635	An issue discovered in MEGAFEIS, BOFEI DBD+ Application for IOS & Android v1.4.4 allows attacker to gain access to sensitive account information via insecure pas
CVE-2023-26284	IBM MQ Certified Container 9.3.0.1 through 9.3.0.3 and 9.3.1.0 through 9.3.1.1 could allow authenticated users with the cluster to be granted administration access to t console due to improper access controls. IBM X-Force ID: 248417.
CVE-2023-25804	Roxy-WI is a Web interface for managing Haproxy, Nginx, Apache, and Keepalived servers. Versions prior to 6.3.5.0 have a limited path traversal vulnerability. An SSH saved into an unintended location, for example the `/tmp` folder using a payload `../../../../../tmp/test111_dev`. This issue has been fixed in version 6.3.5.0.
CVE-2023-27087	Permissions vulnerabiltiy found in Xuxueli xxl-job v2.2.0, v 2.3.0 and v.2.3.1 allows attacker to obtain sensitive information via the pageList parameter.
CVE-2023-25281	A stack overflow vulnerability exists in pingV4Msg component in D-Link DIR820LA1_FW105B03, allows attackers to cause a denial of service via the nextPage parame ping.ccp.
CVE-2023-28450	An issue was discovered in Dnsmasq before 2.90. The default maximum EDNS.0 UDP packet size was set to 4096 but should be 1232 because of DNS Flag Day 2020
CVE-2022-34416	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2022-34415	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2022-34414	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.

CVE Number	Description
CVE-2022-34417	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2022-34406	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2022-34413	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2022-34407	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2022-34408	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2023-1444	A vulnerability was found in Filseclab Twister Antivirus 8. It has been rated as critical. This issue affects the function 0x8011206B in the library fildds.sys of the compon IoControlCode Handler. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be use identifier VDB-223289 was assigned to this vulnerability.
CVE-2022-34410	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2023-24571	Dell BIOS contains an Improper Input Validation vulnerability. A local authenticated malicious user with administrator privileges could potentially exploit this vulnerability arbitrary code execution.
CVE-2022-34411	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2022-34412	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges ma exploit this vulnerability to perform arbitrary code execution or cause denial of service.
CVE-2021-21548	Dell EMC Unisphere for PowerMax versions before 9.1.0.27, Dell EMC Unisphere for PowerMax Virtual Appliance versions before 9.1.0.27, and PowerMax OS Releas contain an improper certificate validation vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability to carry out a man-in-the-middle atta supplying a crafted certificate and intercepting the victim's traffic to view or modify a victim’s data in transit.
CVE-2023-1250	Improper Input Validation vulnerability in OTRS AG OTRS (ACL modules), OTRS AG ((OTRS)) Community Edition (ACL modules) allows Local Execution of Code. Wh creating/importing an ACL it was possible to inject code that gets executed via manipulated comments and ACL-names This issue affects OTRS: from 7.0.X before 7.0 8.0.X before 8.0.31; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34.
CVE-2023-1432	A vulnerability was found in SourceCodester Online Food Ordering System 2.0 and classified as critical. Affected by this issue is some unknown functionality of the file /fos/admin/ajax.php?action=save_settings of the component POST Request Handler. The manipulation leads to improper access controls. The attack may be launchec VDB-223214 is the identifier assigned to this vulnerability.
CVE-2012-10009	A vulnerability was found in 404like Plugin up to 1.0.2 on WordPress. It has been classified as critical. Affected is the function checkPage of the file 404Like.php. The m of the argument searchWord leads to sql injection. It is possible to launch the attack remotely. Upgrading to version 1.0.2 is able to address this issue. The name of the 2c4b589d27554910ab1fd104ddbec9331b540f7f. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-223404.
CVE-2023-1464	A vulnerability, which was classified as critical, was found in SourceCodester Medicine Tracker System 1.0. This affects an unknown part of the file Users.php?f=save_ manipulation of the argument firstname/middlename/lastname/username/password leads to improper authentication. It is possible to initiate the attack remotely. The as identifier of this vulnerability is VDB-223311.
CVE-2023-22883	Zoom Client for IT Admin Windows installers before version 5.13.5 contain a local privilege escalation vulnerability. A local low-privileged user could exploit this vulnera attack chain during the installation process to escalate their privileges to the SYSTEM user.
CVE-2022-36429	A command execution vulnerability exists in the ubus backend communications functionality of Netgear Orbi Satellite RBS750 4.6.8.5. A specially-crafted JSON object arbitrary command execution. An attacker can send a sequence of malicious packets to trigger this vulnerability.
CVE-2023-27709	SQL injection vulnerability found in DedeCMS v.5.7.106 allows a remote attacker to execute arbitrary code via the rank_* parameter in the /dedestory_catalog.php end
CVE-2023-28460	A command injection vulnerability was discovered in Array Networks APV products. A remote attacker can send a crafted packet after logging into the affected applianc administrator, resulting in arbitrary shell code execution. This is fixed in 8.6.1.262 or newer and 10.4.2.93 or newer.

CVE Number	Description
CVE-2023-27235	An arbitrary file upload vulnerability in the \admin\c\CommonController.php component of Jizhicms v2.4.5 allows attackers to execute arbitrary code via a crafted phtml
CVE-2023-27707	SQL injection vulnerability found in DedeCMS v.5.7.106 allows a remote attacker to execute arbitrary code via the rank_* parameter in the /dede/group_store.php endp
CVE-2023-1172	The Bookly plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the full name value in versions up to, and including, 21.5 due to insufficient input saniti output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected pag
CVE-2022-38452	A command execution vulnerability exists in the hidden telnet service functionality of Netgear Orbi Router RBR750 4.6.8.5. A specially-crafted network request can leac command execution. An attacker can send a network request to trigger this vulnerability.
CVE-2021-36821	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPMU DEV Forminator allows Stored XSS.This issue affec Forminator: from n/a through 1.14.11.
CVE-2022-47592	Reflected Cross-Site Scripting (XSS) vulnerability in Dmytriy.Cooperman MagicForm plugin <= 0.1 versions.
CVE-2023-22682	Reflected Cross-Site Scripting (XSS) vulnerability in Manuel Masia | Pixedelic.Com Camera slideshow plugin <= 1.4.0.1 versions.
CVE-2022-47591	Reflected Cross-Site Scripting (XSS) vulnerability in Mickael Austoni Map Multi Marker plugin <= 3.2.1 versions.
CVE-2023-28466	do_tls_getsockopt in net/tls/tls_main.c in the Linux kernel through 6.2.6 lacks a lock_sock call, leading to a race condition (with a resultant use-after-free or NULL pointe dereference).
CVE-2023-22880	Zoom for Windows clients before version 5.13.3, Zoom Rooms for Windows clients before version 5.13.5 and Zoom VDI for Windows clients before 5.13.1 contain an ir disclosure vulnerability. A recent update to the Microsoft Edge WebView2 runtime used by the affected Zoom clients, transmitted text to Microsoft's online Spellcheck s instead of the local Windows Spellcheck. Updating Zoom remediates this vulnerability by disabling the feature. Updating Microsoft Edge WebView2 Runtime to at least 109.0.1481.0 and restarting Zoom remediates this vulnerability by updating Microsoft's telemetry behavior.
CVE-2023-25134	McAfee Total Protection prior to 16.0.50 may allow an adversary (with full administrative access) to modify a McAfee specific Component Object Model (COM) in the W Registry. This can result in the loading of a malicious payload.
CVE-2023-1467	A vulnerability classified as critical has been found in SourceCodester Student Study Center Desk Management System 1.0. Affected is an unknown function of the file f=delete_img of the component POST Parameter Handler. The manipulation of the argument path with the input C%3A%2Ffoo.txt leads to path traversal. It is possible attack remotely. The exploit has been disclosed to the public and may be used. VDB-223326 is the identifier assigned to this vulnerability.
CVE-2023-26040	Discourse is an open-source discussion platform. Between versions 3.1.0.beta2 and 3.1.0.beta3 of the `tests-passed` branch, editing or responding to a chat message malicious content could lead to a cross-site scripting attack. This issue is patched in version 3.1.0.beta3 of the `tests-passed` branch. There are no known workarounds
CVE-2023-27983	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow deletion of reports from the IGSS project r directory, this would lead to loss of data when an attacker abuses this functionality. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and pric Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).
CVE-2022-38458	A cleartext transmission vulnerability exists in the Remote Management functionality of Netgear Orbi Router RBR750 4.6.8.5. A specially-crafted man-in-the-middle atta to a disclosure of sensitive information.
CVE-2023-27595	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. In version 1.13.0, when Cilium is started, there is a short period when Cilium programs are not attached to the host. During this period, the host does not implement any of Cilium's featureset. This can cause disruption to newly established conne during this period due to the lack of Load Balancing, or can cause Network Policy bypass due to the lack of Network Policy enforcement during the window. This vulner impacts any Cilium-managed endpoints on the node (such as Kubernetes Pods), as well as the host network namespace (including Host Firewall). This vulnerability is f Cilium 1.13.1 or later. Cilium releases 1.12.x, 1.11.x, and earlier are not affected. There are no known workarounds.
CVE-2023-25684	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL stateme could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 247597.
CVE-2023-27873	IBM Aspera Faspex 4.4.2 could allow a remote authenticated attacker to obtain sensitive credential information using specially crafted XML input. IBM X-Force ID: 2496

CVE Number	Description
CVE-2023-27979	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could allow the renaming of files in the IGSS project report directory, lead to denial of service when an attacker sends specific crafted messages to the Data Server TCP port. Affected Products: IGSS Data Server(IGSSdataServer.exe) (V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).
CVE-2022-42334	x86/HVM pinned cache attributes mis-handling T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to whi allow cachability control for HVM guests with passed through devices, an interface exists to explicitly override defaults which would otherwise be put in place. While not the affected guests themselves, the interface specifically exists for domains controlling such guests. This interface may therefore be used by not fully privileged entities, running deprivileged in Dom0 or qemu running in a so called stub-domain. With this exposure it is an issue that - the number of the such controlled regions was unbour 2022-42333), - installation and removal of such regions was not properly serialized (CVE-2022-42334).
CVE-2023-0911	The WordPress Shortcodes Plugin — Shortcodes Ultimate WordPress plugin before 5.12.8 does not validate the user meta to be retrieved via the user shortcode, allow authenticated users such as subscriber to retrieve arbitrary user meta (except the user_pass), such as the user email and activation key by default.
CVE-2023-0890	The WordPress Shortcodes Plugin — Shortcodes Ultimate WordPress plugin before 5.12.8 does not ensure that posts to be displayed via some shortcodes are already can be accessed by the user making the request, allowing any authenticated users such as subscriber to view draft, private or even password protected posts. It is also leak the password of protected posts
CVE-2023-27977	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause access to delete files in the IGSS project report director lead to loss of data when an attacker sends specific crafted messages to the Data Server TCP port. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0. prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).
CVE-2023-1460	A vulnerability was found in SourceCodester Online Pizza Ordering System 1.0. It has been classified as critical. This affects an unknown part of the file admin/ajax.php action=save_user of the component Password Change Handler. The manipulation leads to improper authentication. It is possible to initiate the attack remotely. The ide 223305 was assigned to this vulnerability.
CVE-2023-27234	A Cross-Site Request Forgery (CSRF) in /Sys/index.html of Jizhicms v2.4.5 allows attackers to arbitrarily make configuration changes within the application.
CVE-2023-1443	A vulnerability was found in Filseclab Twister Antivirus 8. It has been declared as problematic. This vulnerability affects the function 0x80112053 in the library fildds.sys component IoControlCode Handler. The manipulation leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and r used. The identifier of this vulnerability is VDB-223288.
CVE-2023-27102	Libde265 v1.0.11 was discovered to contain a segmentation violation via the function decoder_context::process_slice_segment_header at decctx.cc.
CVE-2023-28109	Play With Docker is a browser-based Docker playground. Versions 0.0.2 and prior are vulnerable to domain hijacking. Because CORS configuration was not correct, ar could use `play-with-docker.com` as an example and set the origin header in an http request as `evil-play-with-docker.com`. The domain would echo in response heade successfully bypassed the CORS policy and retrieved basic user information. This issue has been fixed in commit ed82247c9ab7990ad76ec2bf1498c2b2830b6f1a. Th known workarounds.
CVE-2023-22882	Zoom clients before version 5.13.5 contain a STUN parsing vulnerability. A malicious actor could send specially crafted UDP traffic to a victim Zoom client to remotely c client to crash, causing a denial of service.
CVE-2023-22881	Zoom clients before version 5.13.5 contain a STUN parsing vulnerability. A malicious actor could send specially crafted UDP traffic to a victim Zoom client to remotely c client to crash, causing a denial of service.
CVE-2023-27095	Insecure Permissions vulnerability found in OpenGoofy Hippo4j v.1.4.3 allows attacker toescalate privileges via the AddUser method of the UserController function in T Management module.
CVE-2023-25282	A heap overflow vulnerability in D-Link DIR820LA1_FW106B02 allows attackers to cause a denial of service via the config.log_to_syslog and log_opt_dropPackets para mydlink_api.ccp.
CVE-2022-4933	A vulnerability, which was classified as critical, has been found in ATM Consulting dolibarr_module_quicksupplierprice up to 1.1.6. Affected by this issue is the function of the file script/interface.php. The manipulation leads to sql injection. The attack may be launched remotely. Upgrading to version 1.1.7 is able to address this issue. Th identified as ccad1e4282b0e393a32fcc852e82ec0e0af5446f. It is recommended to upgrade the affected component. VDB-223382 is the identifier assigned to this vulne
CVE-2023-1472	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missin incorrect nonce validation on its AJAX actions. This makes it possible for unauthenticated attackers to invoke those functions, via forged request granted they can trick administrator into performing an action such as clicking on a link. Actions include resetting the API key, accessing or deleting log files, and deleting cache among others
CVE-2023-1474	A vulnerability classified as critical was found in SourceCodester Automatic Question Paper Generator System 1.0. This vulnerability affects unknown code of the file users/question_papers/manage_question_paper.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223336.
CVE-2023-1475	A vulnerability, which was classified as critical, has been found in SourceCodester Canteen Management System 1.0. This issue affects the function query of the file createuser.php. The manipulation of the argument uemail leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and r used. The identifier VDB-223337 was assigned to this vulnerability.

CVE Number	Description
CVE-2023-1494	A vulnerability classified as critical has been found in IBOS 4.5.5. Affected is an unknown function of the file ApiController.php. The manipulation of the argument emaili 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-22338
CVE-2023-1501	A vulnerability, which was classified as critical, was found in RockOA 2.3.2. This affects the function runAction of the file acloudCosAction.php.SQL. The manipulation c argument fileid 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 VD was assigned to this vulnerability.
CVE-2023-1499	A vulnerability classified as critical was found in code-projects Simple Art Gallery 1.0. Affected by this vulnerability is an unknown functionality of the file adminHome.ph manipulation of the argument reach_city leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Th identifier of this vulnerability is VDB-223399.
CVE-2023-1479	A vulnerability classified as critical has been found in SourceCodester Simple Music Player 1.0. Affected is an unknown function of the file save_music.php. The manipu argument filename leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-22336 identifier assigned to this vulnerability.
CVE-2023-1480	A vulnerability classified as critical was found in SourceCodester Monitoring of Students Cyber Accounts System 1.0. Affected by this vulnerability is an unknown functi file login.php of the component POST Parameter Handler. The manipulation of the argument un leads to sql injection. The attack can be launched remotely. The exploit disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223363.
CVE-2023-1498	A vulnerability classified as critical has been found in code-projects Responsive Hotel Site 1.0. Affected is an unknown function of the file messages.php of the compon Newsletter Log Handler. The manipulation of the argument title leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the may be used. VDB-223398 is the identifier assigned to this vulnerability.
CVE-2023-1497	A vulnerability was found in SourceCodester Simple and Nice Shopping Cart Script 1.0. It has been rated as critical. This issue affects some unknown processing of the uploaderm.php. The manipulation of the argument submit leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the publ be used. The identifier VDB-223397 was assigned to this vulnerability.
CVE-2023-1483	A vulnerability has been found in XiaoBingBy TeaCMS up to 2.0.2 and classified as critical. This vulnerability affects unknown code of the file /admin/getallarticleinfo. T manipulation of the argument searchInfo leads to sql injection. The attack can be initiated remotely. VDB-223366 is the identifier assigned to this vulnerability.
CVE-2023-1484	A vulnerability was found in xzjie cms up to 1.0.3 and classified as critical. This issue affects some unknown processing of the file /api/upload. The manipulation of the uploadFile leads to unrestricted upload. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-223367.
CVE-2022-26080	Use of Insufficiently Random Values vulnerability in ABB Pulsar Plus System Controller NE843_S, ABB Infinity DC Power Plant.This issue affects Pulsar Plus System NE843_S : comcode 150042936; Infinity DC Power Plant: H5692448 G104 G842 G224L G630-4 G451C(2) G461(2) – comcode 150047415.
CVE-2023-1495	A vulnerability classified as critical was found in Rebuild up to 3.2.3. Affected by this vulnerability is the function queryListOfConfig of the file /admin/robot/approval/list. manipulation of the argument q leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifie patch is c9474f84e5f376dd2ade2078e3039961a9425da7. It is recommended to apply a patch to fix this issue. The identifier VDB-223381 was assigned to this vulnera
CVE-2023-1459	A vulnerability was found in SourceCodester Canteen Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file changeUsername.php. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the may be used. The identifier of this vulnerability is VDB-223304.
CVE-2023-1416	A vulnerability classified as critical has been found in Simple Art Gallery 1.0. Affected is an unknown function of the file adminHome.php. The manipulation of the argum social_facebook 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 v VDB-223128.
CVE-2023-1439	A vulnerability, which was classified as critical, has been found in SourceCodester Medicine Tracker System 1.0. This issue affects some unknown processing of the fil medicines/view_details.php of the component GET Parameter Handler. The manipulation of the argument GET leads to sql injection. The attack may be initiated remot exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223283.
CVE-2023-1454	A vulnerability classified as critical has been found in jeecg-boot 3.5.0. This affects an unknown part of the file jmreport/qurestSql. The manipulation of the argument ap 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 associated identifier of this vulnera VDB-223299.
CVE-2023-1468	A vulnerability classified as critical was found in SourceCodester Student Study Center Desk Management System 1.0. Affected by this vulnerability is an unknown func the file admin/?page=reports&date_from=2023-02-17&date_to=2023-03-17 of the component Report Handler. The manipulation of the argument date_from/date_to lea injection. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-223327.
CVE-2023-1440	A vulnerability, which was classified as critical, was found in SourceCodester Automatic Question Paper Generator System 1.0. Affected is an unknown function of the users/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 r exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223284.
CVE-2023-1466	A vulnerability was found in SourceCodester Student Study Center Desk Management System 1.0. It has been rated as critical. This issue affects the function view_stu file admin/?page=students/view_student. The manipulation of the argument id with the input 3' AND (SELECT 2100 FROM (SELECT(SLEEP(5)))FWIC) AND 'butz'='bu sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223325 was assigned to this vulne
CVE-2023-1441	A vulnerability has been found in SourceCodester Automatic Question Paper Generator System 1.0 and classified as critical. Affected by this vulnerability is an unknow functionality of the file admin/courses/view_course.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attac launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223285 was assigned to this vulnerability.

CVE Number	Description
CVE-2018-25082	A vulnerability was found in zwczou WeChat SDK Python 0.3.0 and classified as critical. This issue affects the function validate/to_xml. The manipulation leads to xml e entity reference. The attack may be initiated remotely. Upgrading to version 0.5.5 is able to address this issue. The patch is named e54abadc777715b6dcb545c13214d1dea63df6c9. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-223403.
CVE-2023-1461	A vulnerability was found in SourceCodester Canteen Management System 1.0. It has been declared as critical. This vulnerability affects the function query of the file createCategories.php. The manipulation of the argument categoriesStatus leads to sql injection. The attack can be initiated remotely. VDB-223306 is the identifier assi vulnerability.
CVE-2023-1379	A vulnerability was found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. It has been rated as critical. This issue affects some unknown pro the file addmem.php of the component POST Parameter Handler. The manipulation of the argument firstname leads to sql injection. The attack may be initiated remote exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223127.
CVE-2023-1415	A vulnerability was found in Simple Art Gallery 1.0. It has been declared as critical. This vulnerability affects the function sliderPicSubmit of the file adminHome.php. Th manipulation leads to unrestricted upload. The attack can be initiated remotely. VDB-223126 is the identifier assigned to this vulnerability.
CVE-2023-25686	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force I
CVE-2023-28428	PDFio is a C library for reading and writing PDF files. In versions 1.1.0 and prior, a denial of service vulnerability exists in the pdfio parser. Crafted pdf files can cause th to run at 100% utilization and never terminate. This is different from CVE-2023-24808. A patch for this issue is available in version 1.1.1.
CVE-2023-21458	Improper privilege management vulnerability in PhoneStatusBarPolicy in System UI prior to SMR Mar-2023 Release 1 allows attacker to turn off Do not disturb via unpr intent.
CVE-2023-0322	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Talent Software UNIS allows Reflected XSS.This issue affects UNI 28376.
CVE-2022-43874	IBM App Connect Enterprise Certified Container 4.1, 4.2, 5.0, 5.1, 5.2, 6.0, 6.1, 6.2, and 7.0 is vulnerable to cross-site scripting. This vulnerability allows users to embe JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 239963.
CVE-2023-28606	js/event-graph.js in MISP before 2.4.169 allows XSS via event-graph node tooltips.
CVE-2023-24278	Squidex before 7.4.0 was discovered to contain a squid.svg cross-site scripting (XSS) vulnerability.
CVE-2023-28607	js/event-graph.js in MISP before 2.4.169 allows XSS via the event-graph relationship tooltip.
CVE-2023-1154	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pacsrapor allows Reflected XSS.This issue affects Pacsrapor: befo
CVE-2023-28106	Pimcore is an open source data and experience management platform. Prior to version 10.5.19, an attacker can use cross-site scripting to send a malicious script to ar unsuspecting user. Users may upgrade to version 10.5.19 to receive a patch or, as a workaround, apply the patch manually.
CVE-2023-1248	Improper Input Validation vulnerability in OTRS AG OTRS (Ticket Actions modules), OTRS AG ((OTRS)) Community Edition (Ticket Actions modules) allows Cross-Sit (XSS).This issue affects OTRS: from 7.0.X before 7.0.42; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34.
CVE-2023-28429	Pimcore is an open source data and experience management platform. Versions prior to 10.5.19 have an unsecured tooltip field in DataObject class definition. This vul 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. Users upgrade to version 10.5.19 or, as a workaround, apply the patch manually.
CVE-2023-28155	The Request package through 2.88.1 for Node.js allows a bypass of SSRF mitigations via an attacker-controller server that does a cross-protocol redirect (HTTP to HT HTTPS to HTTP). NOTE: This vulnerability only affects products that are no longer supported by the maintainer.
CVE-2023-0876	The WP Meta SEO WordPress plugin before 4.5.3 does not authorize several ajax actions, allowing low-privilege users to make updates to certain data and leading to redirect vulnerability.
CVE-2023-0937	The VK All in One Expansion Unit WordPress plugin before 9.87.1.0 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attrib could lead to Reflected Cross-Site Scripting in old web browsers

CVE Number	Description
CVE-2023-21453	Improper input validation vulnerability in SoftSim TA prior to SMR Mar-2023 Release 1 allows local attackers access to protected data.
CVE-2023-28098	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, a specially crafted Authorization header causes OpenSIPS to behave in an unexpected way due to a bug in the function `parse_param_name()` . This issue was discovered while performing coverage guided fuzzing of the functior The AddressSanitizer identified that the issue occurred in the function `q_memchr()` which is being called by the function `parse_param_name()`. This issue may cause program behaviour or a server crash. It affects configurations containing functions that make use of the affected code, such as the function `www_authorize()` . Version 3.2.4 contain a fix.
CVE-2023-24381	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in NsThemes Advanced Social Pixel plugin <= 2.1.1 versions.
CVE-2023-25064	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Matteo Candura WP htpasswd plugin <= 1.7 versions.
CVE-2023-25794	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Mighty Digital Nooz plugin <= 1.6.0 versions.
CVE-2023-25795	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in WP-master.Ir Feed Changer & Remover plugin <= 0.2 versions.
CVE-2023-22679	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Nicolas Lemoine WP Better Emails plugin <= 0.4 versions.
CVE-2023-22680	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Altanic No API Amazon Affiliate plugin <= 4.2.2 versions.
CVE-2023-28099	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.9 and 3.2.6, if `ds_is_in_list()` is used with an invalid IP address string (`NU input), OpenSIPS will attempt to print a string from a random address (stack garbage), which could lead to a crash. All users of `ds_is_in_list()` without the `$si` variable parameter could be affected by this vulnerability to a larger, lesser or no extent at all, depending if the data passed to the function is a valid IPv4 or IPv6 address string will are available starting with the 3.1.9 and 3.2.6 minor releases. There are no known workarounds.
CVE-2023-21455	Improper authorization implementation in Exynos baseband prior to SMR Mar-2023 Release 1 allows incorrect handling of unencrypted message.
CVE-2023-25782	Auth. (admin+) vulnerability in Second2none Service Area Postcode Checker plugin <= 2.0.8 versions.
CVE-2023-23718	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Esstat17 Page Loading Effects plugin <= 2.0.0 versions.
CVE-2023-28112	Discourse is an open-source discussion platform. Prior to version 3.1.0.beta3 of the `beta` and `tests-passed` branches, some user provided URLs were being passed FastImage without SSRF protection. Insufficient protections could enable attackers to trigger outbound network connections from the Discourse server to private IP adc affects any site running the `tests-passed` or `beta` branches versions 3.1.0.beta2 and prior. This issue is patched in version 3.1.0.beta3 of the `beta` and `tests-passec There are no known workarounds.
CVE-2023-28113	russh is a Rust SSH client and server library. Starting in version 0.34.0 and prior to versions 0.36.2 and 0.37.1, Diffie-Hellman key validation is insufficient, which can le insecure shared secrets and therefore breaks confidentiality. Connections between a russh client and server or those of a russh peer with some other misbehaving pee likely to be problematic. These may vulnerable to eavesdropping. Most other implementations reject such keys, so this is mainly an interoperability issue in such a case is fixed in versions 0.36.2 and 0.37.1
CVE-2023-27494	Streamlit, software for turning data scripts into web applications, had a cross-site scripting (XSS) vulnerability in versions 0.63.0 through 0.80.0. Users of hosted Stream were vulnerable to a reflected XSS vulnerability. An attacker could craft a malicious URL with Javascript payloads to a Streamlit app. The attacker could then trick the u visiting the malicious URL and, if successful, the server would render the malicious javascript payload as-is, leading to XSS. Version 0.81.0 contains a patch for this vul
CVE-2023-28111	Discourse is an open-source discussion platform. Prior to version 3.1.0.beta3 of the `beta` and `tests-passed` branches, attackers are able to bypass Discourse's serve request forgery (SSRF) protection for private IPv4 addresses by using a IPv4-mapped IPv6 address. The issue is patched in the latest beta and tests-passed version of version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds.
CVE-2023-28110	Jumpserver is a popular open source bastion host, and Koko is a Jumpserver component that is the Go version of coco, refactoring coco's SSH/SFTP service and Web service. Prior to version 2.28.8, using illegal tokens to connect to a Kubernetes cluster through Koko can result in the execution of dangerous commands that may disru container environment and affect normal usage. The vulnerability has been fixed in v2.28.8.
CVE-2020-4927	A vulnerability in the Spectrum Scale 5.0.5.0 through 5.1.6.1 core component could allow unauthorized access to user data or injection of arbitrary data in the communi protocol. IBM X-Force ID: 191695.

CVE Number	Description
CVE-2023-1455	A vulnerability classified as critical was found in SourceCodester Online Pizza Ordering System 1.0. This vulnerability affects unknown code of the file admin/ajax.php? action=login2 of the component Login Page. The manipulation of the argument email with the input abc%40qq.com' AND (SELECT 9110 FROM (SELECT(SLEEP(5))) 'jFNl'='jFNl leads to sql injection. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has disclosed to the public and may be used. The identifier of this vulnerability is VDB-223300.
CVE-2023-1506	A vulnerability, which was classified as critical, was found in SourceCodester E-Commerce System 1.0. Affected is an unknown function of the file login.php. The manip the argument U_USERNAME leads to sql injection. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be exploit has been disclosed to the public and may be used. VDB-223410 is the identifier assigned to this vulnerability.
CVE-2023-1504	A vulnerability classified as critical was found in SourceCodester Alphaware Simple E-Commerce System 1.0. This vulnerability affects unknown code. The manipulatio argument email/password with the input test1%40test.com ' AND (SELECT 6077 FROM (SELECT(SLEEP(5)))dltn) AND 'PhRa'='PhRa leads to sql injection. The attac initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The this vulnerability is VDB-223408.
CVE-2023-1503	A vulnerability classified as critical has been found in SourceCodester Alphaware Simple E-Commerce System 1.0. This affects an unknown part of the file admin/admi The manipulation of the argument username/password with the input admin' AND (SELECT 8062 FROM (SELECT(SLEEP(5)))meUD)-- hLiX leads to sql injection. It is initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be us associated identifier of this vulnerability is VDB-223407.
CVE-2023-1502	A vulnerability was found in SourceCodester Alphaware Simple E-Commerce System 1.0. It has been rated as critical. Affected by this issue is some unknown function file function/edit_customer.php. The manipulation of the argument firstname/mi/lastname with the input a' RLIKE SLEEP(5) AND 'dAbu'='dAbu leads to sql injection. Th be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used 223406 is the identifier assigned to this vulnerability.
CVE-2023-1493	A vulnerability was found in Max Secure Anti Virus Plus 19.0.2.1. It has been rated as problematic. This issue affects the function 0x220019 in the library MaxProctetor component IoControlCode Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to th may be used. The associated identifier of this vulnerability is VDB-223379.
CVE-2022-41696	Versions of VISAM VBASE Automation Base prior to 11.7.5 may disclose information if a valid user opens a specially crafted file.
CVE-2023-21465	Improper access control vulnerability in BixbyTouch prior to version 3.2.02.5 in China models allows untrusted applications access local files.
CVE-2023-1492	A vulnerability was found in Max Secure Anti Virus Plus 19.0.2.1. It has been declared as problematic. This vulnerability affects the function 0x220019 in the library Max of the component IoControlCode Handler. The manipulation of the argument SystemBuffer leads to denial of service. Attacking locally is a requirement. The exploit has disclosed to the public and may be used. VDB-223378 is the identifier assigned to this vulnerability.
CVE-2022-46300	Versions of VISAM VBASE Automation Base prior to 11.7.5 may disclose information if a valid user opens a specially crafted file.
CVE-2022-42331	x86: speculative vulnerability in 32bit SYSCALL path Due to an oversight in the very original Spectre/Meltdown security work (XSA-254), one entrypath performs its spe safety actions too late. In some configurations, there is an unprotected RET instruction which can be attacked with a variety of speculative attacks.
CVE-2022-45121	Versions of VISAM VBASE Automation Base prior to 11.7.5 may disclose information if a valid user opens a specially crafted file.
CVE-2023-1446	A vulnerability classified as problematic was found in Watchdog Anti-Virus 1.4.214.0. Affected by this vulnerability is the function 0x80002004/0x80002008 in the library driver.sys of the component IoControlCode Handler. The manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclose public and may be used. The associated identifier of this vulnerability is VDB-223291.
CVE-2022-45468	Versions of VISAM VBASE Automation Base prior to 11.7.5 may disclose information if a valid user opens a specially crafted file.
CVE-2022-46286	Versions of VISAM VBASE Automation Base prior to 11.7.5 may disclose information if a valid user opens a specially crafted file.
CVE-2022-45155	An Improper Handling of Exceptional Conditions vulnerability in obs-service-go_modules of openSUSE Factory allows attackers that can influence the call to the servic files and directories on the system of the victim. This issue affects: SUSE openSUSE Factory obs-service-go_modules versions prior to 0.6.1.
CVE-2023-28425	Redis is an in-memory database that persists on disk. Starting in version 7.0.8 and prior to version 7.0.10, authenticated users can use the MSETNX command to trigg assertion and termination of the Redis server process. The problem is fixed in Redis version 7.0.10.
CVE-2023-1487	A vulnerability, which was classified as problematic, has been found in Lespeed WiseCleaner Wise System Monitor 1.5.3.54. This issue affects the function 0x9C40208C/0x9C402000/0x9C402084/0x9C402088/0x9C402004/0x9C4060C4/0x9C4060CC/0x9C4060D0/0x9C4060D4/0x9C40A0DC/0x9C40A0D8/0x9C40A0DC/ in the library WiseHDInfo64.dll of the component IoControlCode Handler. The manipulation leads to denial of service. Attacking locally is a requirement. The exploit has disclosed to the public and may be used. The identifier VDB-223373 was assigned to this vulnerability.

CVE Number	Description
CVE-2022-43512	Versions of VISAM VBASE Automation Base prior to 11.7.5 may disclose information if a valid user opens a specially crafted file.
CVE-2023-0167	The GetResponse for WordPress plugin through 5.5.31 does not validate and escape some of its shortcode attributes before outputting them back in a page/post wher shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
CVE-2023-1515	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.19.
CVE-2022-46854	Cross-Site Request Forgery (CSRF) vulnerability in Obox Themes Launchpad – Coming Soon & Maintenance Mode plugin <= 1.0.13 versions.
CVE-2022-41831	Auth. (contributor+) Cross-Site Scripting vulnerability in TCBarrett WP Glossary plugin <= 3.1.2 versions.
CVE-2022-41785	Auth. (contributor+) Stored Cross-Site Scripting vulnerability in Galleryape Gallery Images Ape plugin <= 2.2.8 versions.
CVE-2022-40699	Cross-Site Scripting (XSS) vulnerability in Dario Curvino Yasr – Yet Another Stars Rating plugin <= 3.1.2 versions.
CVE-2023-0145	The Saan World Clock WordPress plugin through 1.8 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where t shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
CVE-2023-0273	The Custom Content Shortcode WordPress plugin through 4.0.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/p the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks
CVE-2023-0175	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them b page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
CVE-2022-46774	IBM Manage Application 8.8.0 and 8.9.0 in the IBM Maximo Application Suite is vulnerable to incorrect default permissions which could give access to a user to actions should not have access to. IBM X-Force ID: 242953.
CVE-2023-1542	Business Logic Errors in GitHub repository answerdev/answer prior to 1.0.6.
CVE-2023-0364	The real.Kit WordPress plugin before 5.1.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortco embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
CVE-2023-0365	The React Webcam WordPress plugin through 1.2.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where th is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
CVE-2022-42485	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Galaxy Weblinks Gallery with thumbnail slider plugin <= 6.0 versions.
CVE-2023-0370	The WPB Advanced FAQ WordPress plugin through 1.0.6 does not validate and escape some of its shortcode attributes before outputting them back in a page/post wh shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
CVE-2023-1536	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.7.
CVE-2022-45817	Cross-Site Scripting (XSS) vulnerability in Erin Garscadden GC Testimonials plugin <= 1.3.2 versions.
CVE-2023-1535	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.7.

CVE Number	Description
CVE-2023-1527	Cross-site Scripting (XSS) - Generic in GitHub repository tsolucio/corebos prior to 8.0.
CVE-2023-0369	The GoToWP WordPress plugin through 5.1.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the sho embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
CVE-2022-45814	Stored Cross-Site Scripting (XSS) vulnerability in Fabian von Allmen WP Calendar plugin <= 1.5.3 versions.
CVE-2023-0320	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Izmir Katip Celebi University UBYS allows Stored XSS.This issue a UBYS: before 23.03.16.
CVE-2023-27059	A cross-site scripting (XSS) vulnerability in the Edit Group function of ChurchCRM v4.5.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payloa into the Edit Group Name text field.
CVE-2023-1429	Cross-site Scripting (XSS) - Reflected in GitHub repository pimcore/pimcore prior to 10.5.19.
CVE-2023-22678	Cross-Site Request Forgery (CSRF) vulnerability in Rafael Dery Superior FAQ plugin <= 1.0.2 versions.
CVE-2023-25709	Cross-Site Request Forgery (CSRF) vulnerability in Plainware Locatoraid Store Locator plugin <= 3.9.11 versions.
CVE-2023-1496	Cross-site Scripting (XSS) - Reflected in GitHub repository imgproxy/imgproxy prior to 3.14.0.
CVE-2023-26951	onekeyadmin v1.3.9 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Member List module.
CVE-2023-1463	Authorization Bypass Through User-Controlled Key in GitHub repository nilsteampassnet/teampass prior to 3.0.0.23.
CVE-2022-47427	Cross-Site Request Forgery (CSRF) vulnerability in Joseph C Dolson My Calendar plugin <= 3.3.24.1 versions.
CVE-2022-38063	Cross-Site Request Forgery (CSRF) vulnerability in Social Login WP plugin <= 5.0.0.0 versions.
CVE-2023-1540	Observable Response Discrepancy in GitHub repository answerdev/answer prior to 1.0.6.
CVE-2023-1452	A vulnerability was found in GPAC 2.3-DEV-rev35-gbbca86917-master. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the filters/load_text.c. The manipulation leads to buffer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be recommended to apply a patch to fix this issue. The identifier VDB-223297 was assigned to this vulnerability.
CVE-2023-1431	The WP Simple Shopping Cart plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 4.6.3 due to the plugin saving sho data exports in a publicly accessible location (/wp-content/plugins/wordpress-simple-paypal-shopping-cart/includes/admin/). This makes it possible for unauthenticated view information that should be limited to administrators only and can include data like first name, last name, email, address, IP Address, and more.
CVE-2023-1449	A vulnerability has been found in GPAC 2.3-DEV-rev35-gbbca86917-master and classified as problematic. This vulnerability affects the function gf_av1_reset_state of media_tools/av_parsers.c. The manipulation leads to double free. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and It is recommended to apply a patch to fix this issue. VDB-223294 is the identifier assigned to this vulnerability.
CVE-2023-1538	Observable Timing Discrepancy in GitHub repository answerdev/answer prior to 1.0.6.
CVE-2023-1539	Improper Restriction of Excessive Authentication Attempts in GitHub repository answerdev/answer prior to 1.0.6.

CVE Number	Description
CVE-2023-25695	Generation of Error Message Containing Sensitive Information vulnerability in Apache Software Foundation Apache Airflow.This issue affects Apache Airflow: before 2.
CVE-2023-28486	Sudo before 1.9.13 does not escape control characters in log messages.
CVE-2023-1448	A vulnerability, which was classified as problematic, was found in GPAC 2.3-DEV-rev35-gbbca86917-master. This affects the function gf_m2ts_process_sdt of the file media_tools/mpegts.c. The manipulation leads to heap-based buffer overflow. Attacking locally is a requirement. The exploit has been disclosed to the public and may recommended to apply a patch to fix this issue. The identifier VDB-223293 was assigned to this vulnerability.
CVE-2023-28487	Sudo before 1.9.13 does not escape control characters in sudoreplay output.
CVE-2023-0027	Rockwell Automation Modbus TCP Server AOI prior to 2.04.00 is vulnerable to an unauthorized user sending a malformed message that could cause the controller to r a copy of the most recent response to the last valid request. If exploited, an unauthorized user could read the connected device's Modbus TCP Server AOI information.
CVE-2023-27084	Permissions vulnerability found in isoftforce Dreamer CMS v.4.0.1 allows local attackers to obtain sensitive information via the AttachmentController parameter.
CVE-2015-10096	A vulnerability, which was classified as critical, was found in Zarthus IRC Twitter Announcer Bot up to 1.1.0. This affects the function get_tweets of the file lib/twitterbot/plugins/twitter_announcer.rb. The manipulation of the argument tweet leads to command injection. It is possible to initiate the attack remotely. The complex attack is rather high. The exploitability is told to be difficult. Upgrading to version 1.1.1 is able to address this issue. The patch is named 6b1941b7fc2c70e1f40981b43c84a2c20cc12bd3. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-223383.
CVE-2023-28101	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. In versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4, if an attacker Flatpak app with elevated permissions, they can hide those permissions from users of the `flatpak(1)` command-line interface by setting other permissions to crafted va contain non-printable control characters such as `ESC`. A fix is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, use a GUI like GNOME Softw than the command-line interface, or only install apps whose maintainers you trust.
CVE-2023-1505	A vulnerability, which was classified as critical, has been found in SourceCodester E-Commerce System 1.0. This issue affects some unknown processing of the file /ecommerce/admin/settings/setDiscount.php. The manipulation of the argument id with the input 201737 AND (SELECT 8973 FROM (SELECT(SLEEP(5)))OoAD) lead injection. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the may be used. The identifier VDB-223409 was assigned to this vulnerability.
CVE-2023-21459	Use after free vulnerability in decon driver prior to SMR Mar-2023 Release 1 allows attackers to cause memory access fault.
CVE-2022-37402	Stored Cross-site Scripting (XSS) vulnerability in AFS Analytics plugin <= 4.18 versions.
CVE-2022-41554	Stored Cross-Site Scripting (XSS) vulnerability in John West Slideshow SE plugin <= 2.5.5 versions.
CVE-2023-26912	Cross site scripting (XSS) vulnerability in xenv S-mall-ssm thru commit 3d9e77f7d80289a30f67aaba1ae73e375d33ef71 on Feb 17, 2020, allows local attackers to exec code via the evaluate button.
CVE-2022-43461	Stored Cross-Site Scripting (XSS) vulnerability in John West Slideshow SE plugin <= 2.5.5 versions.
CVE-2023-1517	Cross-site Scripting (XSS) - DOM in GitHub repository pimcore/pimcore prior to 10.5.19.
CVE-2023-27130	Cross Site Scripting vulnerability found in Typecho v.1.2.0 allows a remote attacker to execute arbitrary code via an arbitrarily supplied URL parameter.
CVE-2023-27131	Cross Site Scripting vulnerability found in Typecho v.1.2.0 allows a remote attacker to execute arbitrary code viathe Post Editorparameter.
CVE-2023-27711	Cross Site Scripting vulnerability found in Typecho v.1.2.0 allows a remote attacker to execute arbitrary code via the Comment Manager /admin/manage-comments.php component.

CVE Number	Description
CVE-2023-27592	Miniflux is a feed reader. Since v2.0.25, Miniflux will automatically proxy images served over HTTP to prevent mixed content errors. When an outbound request made b HTTP client fails, the `html.ServerError` is returned unescaped without the expected Content Security Policy header added to valid responses. By creating an RSS feec the inline description containing an `<img>` tag with a `srcset` attribute pointing to an invalid URL like `http:a<script>alert(1)</script>`, we can coerce the proxy handler condition where the invalid URL is returned unescaped and in full. This results in JavaScript execution on the Miniflux instance as soon as the user is convinced (e.g. by in the alt text) to open the broken image. An attacker can execute arbitrary JavaScript in the context of a victim Miniflux user when they open a broken image in a crafte This can be used to perform actions on the Miniflux instance as that user and gain administrative access to the Miniflux instance if it is reachable and the victim is an ac A patch is available in version 2.0.43. As a workaround sisable image proxy; default value is `http-only`.
CVE-2022-34148	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JetBackup JetBackup – WP Backup, Migrate & Restore plugin <= 1 versions.
CVE-2023-1442	A vulnerability was found in Meizhou Qingyunke QYKCMS 4.3.0. It has been classified as problematic. This affects an unknown part of the file /admin_system/api.php c component Update Handler. The manipulation of the argument downurl leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been d the public and may be used. The associated identifier of this vulnerability is VDB-223287.
CVE-2023-1407	A vulnerability classified as critical was found in SourceCodester Student Study Center Desk Management System 1.0. Affected by this vulnerability is an unknown func the file /admin/user/manage_user.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed public and may be used. The associated identifier of this vulnerability is VDB-223111.
CVE-2023-1433	A vulnerability was found in SourceCodester Gadget Works Online Ordering System 1.0. It has been classified as problematic. This affects an unknown part of the file admin/products/controller.php?action=add of the component Products Handler. The manipulation of the argument filename leads to unrestricted upload. It is possible tc attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223215.
CVE-2023-1482	A vulnerability, which was classified as problematic, was found in HkCms 2.2.4.230206. This affects an unknown part of the file /admin.php/appcenter/local.html?type=a component External Plugin Handler. The manipulation leads to code injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public a used. The identifier VDB-223365 was assigned to this vulnerability.
CVE-2022-38971	Stored Cross-Site Scripting (XSS) vulnerability in ThemeKraft Post Form – Registration Form – Profile Form for User Profiles and Content Forms for User Submissions <= 2.7.5 versions.
CVE-2023-28096	OpenSIPS, a Session Initiation Protocol (SIP) server implementation, has a memory leak starting in the 2.3 branch and priot to versions 3.1.8 and 3.2.5. The memory le detected in the function `parse_mi_request` while performing coverage-guided fuzzing. This issue can be reproduced by sending multiple requests of the form `{"jsonrp "2.0","method": "log_le`. This malformed message was tested against an instance of OpenSIPS via FIFO transport layer and was found to increase the memory consur time. To abuse this memory leak, attackers need to reach the management interface (MI) which typically should only be exposed on trusted interfaces. In cases where exposed to the internet without authentication, abuse of this issue will lead to memory exhaustion which may affect the underlying system's availability. No authenticatic required to reproduce this issue. On the other hand, memory leaks may occur in other areas of OpenSIPS where the cJSON library is used for parsing JSON objects. T has been fixed in versions 3.1.8 and 3.2.5.
CVE-2023-28107	Discourse is an open-source discussion platform. Prior to version 3.0.2 of the `stable` branch and version 3.1.0.beta3 of the `beta` and `tests-passed` branches, a user an administrator can request backups multiple times, which will eat up all the connections to the DB. If this is done on a site using multisite, then it can affect the whole vulnerability is patched in version 3.0.2 of the `stable` branch and version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds.
CVE-2023-1453	A vulnerability was found in Watchdog Anti-Virus 1.4.214.0. It has been rated as critical. Affected by this issue is the function 0x80002008 in the library wsdk-driver.sys component IoControlCode Handler. The manipulation leads to improper access controls. Attacking locally is a requirement. The exploit has been disclosed to the public be used. VDB-223298 is the identifier assigned to this vulnerability.
CVE-2023-1491	A vulnerability was found in Max Secure Anti Virus Plus 19.0.2.1. It has been classified as critical. This affects the function 0x220020 in the library MaxCryptMon.sys of component IoControlCode Handler. The manipulation leads to improper access controls. Local access is required to approach this attack. The exploit has been disclose public and may be used. The identifier VDB-223377 was assigned to this vulnerability.
CVE-2023-21460	Improper authentication in SecSettings prior to SMR Mar-2023 Release 1 allows attacker to reset the setting.
CVE-2023-25172	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, a malic crafted URL can be included in a user's full name field to to carry out cross-site scripting attacks on sites with a disabled or overly permissive CSP (Content Security Po Discourse's default CSP prevents this vulnerability. The vulnerability is patched in version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-pa branches. As a workaround, enable and/or restore your site's CSP to the default one provided with Discourse.
CVE-2023-1486	A vulnerability classified as problematic was found in Lespeed WiseCleaner Wise Force Deleter 1.5.3.54. This vulnerability affects the function 0x220004 in the library WiseUnlock64.sys of the component IoControlCode Handler. The manipulation leads to improper access controls. Local access is required to approach this attack. The been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223372.
CVE-2023-1490	A vulnerability was found in Max Secure Anti Virus Plus 19.0.2.1 and classified as critical. Affected by this issue is the function 0x220020 in the library SDActMon.sys o component IoControlCode Handler. The manipulation leads to improper access controls. An attack has to be approached locally. The exploit has been disclosed to the may be used. The identifier of this vulnerability is VDB-223376.
CVE-2023-27593	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.11.15, 1.12.8, and 1.13.1, an attacker with access to a Cil pod can write to `/opt/cni/bin` due to a `hostPath` mount of that directory in the agent pod. By replacing the CNI binary with their own malicious binary and waiting for th a new pod on the node, the attacker can gain access to the underlying node. The issue has been fixed and the fix is available on versions 1.11.15, 1.12.8, and 1.13.1. S workarounds are available. Kubernetes RBAC should be used to deny users and service accounts `exec` access to Cilium agent pods. In cases where a user requires access to Cilium agent pods, but should not have access to the underlying node, no workaround is possible.

CVE Number	Description
CVE-2023-1469	The WP Express Checkout plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘pec_coupon[code]’ parameter in versions up to, and including, 2.2 insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with administrator-level access to inject arbitrary web scripts in pag execute whenever a user accesses an injected page. Note: This can potentially be exploited by lower-privileged users if the `Admin Dashboard Access Permission` set those users to access the dashboard.
CVE-2023-1470	The eCommerce Product Catalog plugin for WordPress is vulnerable to Stored Cross-Site Scripting via some of its settings parameters in versions up to, and including, insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary 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 disable
CVE-2022-46773	IBM Robotic Process Automation 21.0.0 - 21.0.7 and 23.0.0 is vulnerable to client-side validation bypass for credential pools. Invalid credential pools may be created a IBM X-Force ID: 242951.
CVE-2023-25687	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to obtain sensitive information from log files. IBM X-Forc 247602.
CVE-2023-0681	Rapid7 InsightVM versions 6.6.178 and lower suffers from an open redirect vulnerability, whereby an attacker has the ability to redirect the user to a site of the attacker using the ‘page’ parameter of the ‘data/console/redirect’ component of the application. This issue was resolved in the February, 2023 release of version 6.6.179.
CVE-2023-25708	Cross-Site Request Forgery (CSRF) vulnerability in Rextheme WP VR – 360 Panorama and Virtual Tour Builder For WordPress plugin <= 8.2.7 versions.
CVE-2023-22681	Cross-Site Request Forgery (CSRF) vulnerability in Aarvanshinfotech Online Exam Software: eExamhall plugin <= 4.0 versions.
CVE-2022-38456	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Ernest Marcinko Ajax Search Lite plugin <= 4.10.3 versions.
CVE-2023-25968	Cross-Site Request Forgery (CSRF) vulnerability in Cozmoslabs, Madalin Ungureanu, Antohe Cristian Client Portal – Private user pages and login plugin <= 1.1.8 vers
CVE-2023-23721	Cross-Site Request Forgery (CSRF) vulnerability in David Gwyer Admin Log plugin <= 1.50 versions.
CVE-2022-46867	Cross-Site Request Forgery (CSRF) vulnerability in Chasil Universal Star Rating plugin <= 2.1.0 version.
CVE-2022-3894	The WP OAuth Server (OAuth Authentication) WordPress plugin before 4.2.5 does not have CSRF check when deleting a client, and does not ensure that the object to is actually a client, which could allow attackers to make a logged in admin delete arbitrary client and post via a CSRF attack.
CVE-2022-4148	The WP OAuth Server (OAuth Authentication) WordPress plugin before 4.3.0 has a flawed CSRF and authorisation check when deleting a client, which could allow any authenticated users, such as subscriber to delete arbitrary client.
CVE-2023-23622	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the co displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sens determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` an passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to of all topics regardless of the topic's category read restrictions.
CVE-2023-22876	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.7 and 6.1.0.0 through 6.1.2.1 could allow a privileged user to obtain sensitive information that could attacks against the system. IBM X-Force ID: 244364.
CVE-2023-21462	The sensitive information exposure vulnerability in Quick Share Agent prior to versions 3.5.14.18 in Android 12 and 3.5.16.20 in Android 13 allows to local attacker to a address without related permission.
CVE-2023-25680	IBM Robotic Process Automation 21.0.1 through 21.0.5 is vulnerable to insufficiently protecting credentials. Queue Provider credentials are not obfuscated while editing provider details. IBM X-Force ID: 247032.
CVE-2023-27594	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.11.15, 1.12.8, and 1.13.1, under specific conditions, Ciliu misattribute the source IP address of traffic to a cluster, identifying external traffic as coming from the host on which Cilium is running. As a consequence, network polic cluster might be bypassed, depending on the specific network policies enabled. This issue only manifests when Cilium is routing IPv6 traffic and NodePorts are used to to pods. IPv6 and endpoint routes are both disabled by default. The problem has been fixed and is available on versions 1.11.15, 1.12.8, and 1.13.1. As a workaround, routing.

CVE Number	Description
CVE-2023-22288	HTML Email Injection in Tribe29 Checkmk <=2.1.0p23; <=2.0.0p34, and all versions of Checkmk 1.6.0 allows an authenticated attacker to inject malicious HTML into E
CVE-2023-21457	Improper access control vulnerability in Bluetooth prior to SMR Mar-2023 Release 1 allows attackers to send file via Bluetooth without related permission.
CVE-2023-21461	Improper authorization vulnerability in AutoPowerOnOffConfirmDialog in Settings prior to SMR Mar-2023 Release 1 allows local attacker to turn device off via unprotect
CVE-2023-21463	Improper access control vulnerability in MyFiles application prior to versions 12.2.09.0 in Android 11, 13.1.03.501 in Android 12 and 14.1.03.0 in Android 13 allows loca get sensitive information of secret mode in Samsung Internet application with specific conditions.
CVE-2023-21464	Improper access control in Samsung Calendar prior to versions 12.4.02.9000 in Android 13 and 12.3.08.2000 in Android 12 allows local attacker to configure improper
CVE-2023-21449	Improper access control vulnerability in Call application prior to SMR Mar-2023 Release 1 allows local attackers to access sensitive information without proper permissi
CVE-2020-4556	IBM Financial Transaction Manager for High Value Payments for Multi-Platform 3.2.0 through 3.2.10 allows web pages to be stored locally which can be read by anothe the system. IBM X-Force ID: 183329.
CVE-2023-22591	IBM Robotic Process Automation 21.0.1 through 21.0.7 and 23.0.0 through 23.0.1 could allow a user with physical access to the system due to session tokens for not b invalidated after a password reset. IBM X-Force ID: 243710.
CVE-2023-1541	Business Logic Errors in GitHub repository answerdev/answer prior to 1.0.6.
CVE-2023-26084	The armv8_dec_aes_gcm_full() API of Arm AArch64cryptolib before 86065c6 fails to the verify the authentication tag of AES-GCM protected data, leading to a man-in- attack. This occurs because of an improperly initialized variable.
CVE-2023-1421	A reflected cross-site scripting vulnerability in the OAuth flow completion endpoints in Mattermost allows an attacker to send AJAX requests on behalf of the victim via s crafted link with a malicious state parameter.
CVE-2016-15029	A vulnerability has been found in Ydalb mapicoin up to 1.9.0 and classified as problematic. This vulnerability affects unknown code of the file webroot/stats.php. The ma of the argument link/search leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 1.10.0 is able to address this issue. The patch is ide 67e87f0f0c1ac238fcd050f4c3db298229bc9679. It is recommended to upgrade the affected component. VDB-223402 is the identifier assigned to this vulnerability.
CVE-2023-1485	A vulnerability classified as problematic has been found in SourceCodester Young Entrepreneur E-Negosyo System 1.0. This affects an unknown part of the file /bsenordering/index.php of the component GET Parameter Handler. The manipulation of the argument category with the input <script>alert(222)</script> leads to cross 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
CVE-2023-1481	A vulnerability, which was classified as problematic, has been found in SourceCodester Monitoring of Students Cyber Accounts System 1.0. Affected by this issue is so unknown functionality of the file modules/balance/index.php?view=balancelist of the component POST Parameter Handler. The manipulation of the argument id with the <script>alert(111)</script> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The ident vulnerability is VDB-223364.
CVE-2023-1500	A vulnerability, which was classified as problematic, has been found in code-projects Simple Art Gallery 1.0. Affected by this issue is some unknown functionality of the adminHome.php. The manipulation of the argument about_info leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to th may be used. The identifier of this vulnerability is VDB-223400.
CVE-2023-1418	A vulnerability classified as problematic was found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. Affected by this vulnerability is an unkno functionality of the file cashconfirm.php of the component POST Parameter Handler. The manipulation of the argument transactioncode leads to cross site scripting. Th be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223129 was assigned to this vulnerability.
CVE-2023-1507	A vulnerability has been found in SourceCodester E-Commerce System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of th /ecommerce/admin/category/controller.php of the component Category Name Handler. The manipulation of the argument CATEGORY leads to cross site scripting. The be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223411.
CVE-2023-23935	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a resu users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patc versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a an admin may enable the `display_personal_messages_tag_counts` site setting.
CVE-2023-1447	A vulnerability, which was classified as problematic, has been found in SourceCodester Medicine Tracker System 1.0. Affected by this issue is some unknown functiona file app/?page=medicines/manage_medicine. The manipulation of the argument name/description with the input <script>alert('2')</script> leads to cross site scripting. T may be launched remotely. The identifier of this vulnerability is VDB-223292.

CVE Number	Description
CVE-2023-1451	A vulnerability was found in MP4v2 2.1.2. It has been classified as problematic. Affected is the function mp4v2::impl::MP4Track::GetSampleFileOffset of the file mp4tra manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulr VDB-223296.
CVE-2023-21452	Improper usage of implicit intent in Bluetooth prior to SMR Mar-2023 Release 1 allows attacker to get MAC address of connected device.
CVE-2023-1445	A vulnerability classified as problematic has been found in Filseclab Twister Antivirus 8. Affected is the function 0x80112053 in the library fildds.sys of the component IoControlCode Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may b VDB-223290 is the identifier assigned to this vulnerability.
CVE-2023-1450	A vulnerability was found in MP4v2 2.1.2 and classified as problematic. This issue affects the function DumpTrack of the file mp4trackdump.cpp. The manipulation lead of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VD
CVE-2023-1488	A vulnerability, which was classified as problematic, was found in Lespeed WiseCleaner Wise System Monitor 1.5.3.54. Affected is the function 0x9C40A0D8/0x9C40A0DC/0x9C40A0E0 in the library WiseHDInfo64.dll of the component IoControlCode Handler. The manipulation leads to denial of service. It is po launch the attack on the local host. The exploit has been disclosed to the public and may be used. VDB-223374 is the identifier assigned to this vulnerability.
CVE-2023-25923	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an attacker to upload files that could be used in a denial of service attack due authorization. IBM X-Force ID: 247629.
CVE-2023-25689	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1 , and 4.1.1 could allow a remote attacker to traverse directories on the system. An attacker could ser crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 247618.
CVE-2023-21454	Improper authorization in Samsung Keyboard prior to SMR Mar-2023 Release 1 allows physical attacker to access users text history on the lockscreen.
CVE-2023-28426	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: GHSA-xrqq-wqh4-5hg2. Reason: Further investigation showed that this CVE was assigned Notes: See https://github.com/darylldoyle/svg-sanitizer/issues/88 for a technical discussion.