SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 26 July 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-2023-3765	Absolute Path Traversal in GitHub repository mlflow/mlflow prior to 2.5.0.	10.0	More Details
CVE-2023-26045	NodeBB is Node.js based forum software. Starting in version 2.5.0 and prior to version 2.8.7, due to the use of the object destructuring assignment syntax in the user export code path, combined with a path traversal vulnerability, a specially crafted payload could invoke the user export logic to arbitrarily execute javascript files on the local disk. This issue is patched in version 2.8.7. As a workaround, site maintainers can cherry pick the fix into their codebase to patch the exploit.	10.0	More Details
CVE-2023-32231	An issue was discovered in Vasion PrinterLogic Client for Windows before 25.0.0.818. During installation, binaries gets executed out of a subfolder in C:\Windows\Temp. A standard user can create the folder and path file ahead of time and obtain elevated code execution.	9.9	More Details
CVE-2023-32232	An issue was discovered in Vasion PrinterLogic Client for Windows before 25.0.0.836. During client installation and repair, a PrinterLogic binary is called by the installer to configure the device. This window is not hidden, and is running with elevated privileges. A standard user can break out of this window, obtaining a full SYSTEM command prompt window. This results in complete compromise via arbitrary SYSTEM code execution (elevation of privileges).	9.9	More Details
CVE-2022-46290	Multiple out-of-bounds write vulnerabilities exist in the ORCA format nAtoms functionality of Open Babel 3.1.1 and master commit 530dbfa3. A specially-crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.The loop that stores the coordinates does not check its index against nAtoms	9.8	More Details
CVE-2022-46292	Multiple out-of-bounds write vulnerabilities exist in the translationVectors parsing functionality in multiple supported formats of Open Babel 3.1.1 and master commit 530dbfa3. A specially-crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability affects the MOPAC file format, inside the Unit Cell Translation section	9.8	More Details
CVE-2022-46293	Multiple out-of-bounds write vulnerabilities exist in the translationVectors parsing functionality in multiple supported formats of Open Babel 3.1.1 and master commit 530dbfa3. A specially-crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability affects the MOPAC file format, inside the Final Point and Derivatives section	9.8	More Details
CVE-2022-46294	Multiple out-of-bounds write vulnerabilities exist in the translationVectors parsing functionality in multiple supported formats of Open Babel 3.1.1 and master commit 530dbfa3. A specially-crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability affects the MOPAC Cartesian file format	9.8	More Details
CVE-2022-46295	Multiple out-of-bounds write vulnerabilities exist in the translationVectors parsing functionality in multiple supported formats of Open Babel 3.1.1 and master commit 530dbfa3. A specially-crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability affects the Gaussian file format	9.8	More Details
CVE-2023-34478	Apache Shiro, before 1.12.0 or 2.0.0-alpha-3, may be susceptible to a path traversal attack that results in an authentication bypass when used together with APIs or other web frameworks that route requests based on non-normalized requests. Mitigation: Update to Apache Shiro 1.12.0+ or 2.0.0-alpha-3+	9.8	More Details
CVE-2023-32637	GBrowse accepts files with any formats uploaded and places them in the area accessible through unauthenticated web requests. Therefore, anyone who can upload files through the product may execute arbitrary code on the server.	9.8	More Details
CVE-2023-3046	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Biltay Technology Scienta allows SQL Injection.This issue affects Scienta: before 20230630.1953.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35066	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Infodrom Software E-Invoice Approval System allows SQL Injection.This issue affects E-Invoice Approval System: before v.20230701.	9.8	More Details
CVE-2023-35078	An authentication bypass vulnerability in Ivanti EPMM allows unauthorized users to access restricted functionality or resources of the application without proper authentication.	9.8	More Details
CVE-2023-35088	Improper Neutralization of Special Elements Used in an SQL Command ('SQL Injection') vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.7.0. In the toAuditCkSql method, the groupId, streamId, auditId, and dt are directly concatenated into the SQL query statement, which may lead to SQL injection attacks. Users are advised to upgrade to Apache InLong's 1.8.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/8198	9.8	More Details
CVE-2023-37895	Java object deserialization issue in Jackrabbit webapp/standalone on all platforms allows attacker to remotely execute code via RMIVersions up to (including) 2.20.10 (stable branch) and 2.21.17 (unstable branch) use the component "commons-beanutils", which contains a class that can be used for remote code execution over RMI. Users are advised to immediately update to versions 2.20.11 or 2.21.18. Note that earlier stable branches (1.0.x .. 2.18.x) have been EOLd already and do not receive updates anymore. In general, RMI support can expose vulnerabilities by the mere presence of an exploitable class on the classpath. Even if Jackrabbit itself does not contain any code known to be exploitable anymore, adding other components to your server can expose the same type of problem. We therefore recommend to disable RMI access altogether (see further below), and will discuss deprecating RMI support in future Jackrabbit releases. How to check whether RMI support is enabledRMI support can be over an RMI-specific TCP port, and over an HTTP binding. Both are by default enabled in Jackrabbit webapp/standalone. The native RMI protocol by default uses port 1099. To check whether it is enabled, tools like "netstat" can be used to check. RMI-over-HTTP in Jackrabbit by default uses the path "/rmi". So when running standalone on port 8080, check whether an HTTP GET request on localhost:8080/rmi returns 404 (not enabled) or 200 (enabled). Note that the HTTP path may be different when the webapp is deployed in a container as non-root context, in which case the prefix is under the user's control. Turning off RMIFind web.xml (either in JAR/WAR file or in unpacked web application folder), and remove the declaration and the mapping definition for the RemoteBindingServlet: <servlet> <servlet-name>RMI</servlet-name> <servlet-class>org.apache.jackrabbit.servlet.remote.RemoteBindingServlet</servlet-class> </servlet> <servlet-mapping> <servlet-name>RMI</servlet-name> <url-pattern>/rmi</url-pattern> </servlet-mapping> Find the bootstrap.properties file (in $REPOSITORY_HOME), and set rmi.enabled=false and also remove rmi.host rmi.port rmi.url-pattern If there is no file named bootstrap.properties in $REPOSITORY_HOME, it is located somewhere in the classpath. In this case, place a copy in $REPOSITORY_HOME and modify it as explained.	9.8	More Details
CVE-2023-35980	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2023-35981	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2023-35982	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2022-46898	An issue was discovered in Vocera Report Server and Voice Server 5.x through 5.8. There is Path Traversal via the "restore SQL data" filename. The Vocera Report Console contains a websocket function that allows for the restoration of the database from a ZIP archive that expects a SQL import file. The filename provided is not properly sanitized and allows for the inclusion of a path-traversal payload that can be used to escape the intended Vocera restoration directory. An attacker could exploit this vulnerability to point to a crafted ZIP archive that contains SQL commands that could be executed against the database.	9.8	More Details
CVE-2023-34798	An arbitrary file upload vulnerability in eoffice before v9.5 allows attackers to execute arbitrary code via uploading a crafted file.	9.8	More Details
CVE-2022-46291	Multiple out-of-bounds write vulnerabilities exist in the translationVectors parsing functionality in multiple supported formats of Open Babel 3.1.1 and master commit 530dbfa3. A specially-crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability affects the MSI file format	9.8	More Details
CVE-2022-46289	Multiple out-of-bounds write vulnerabilities exist in the ORCA format nAtoms functionality of Open Babel 3.1.1 and master commit 530dbfa3. A specially-crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.nAtoms calculation wrap-around, leading to a small buffer allocation	9.8	More Details
CVE-2023-37292	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in HGiga iSherlock 4.5 (iSherlock-user modules), HGiga iSherlock 5.5 (iSherlock-user modules) allows OS Command Injection.This issue affects iSherlock 4.5: before iSherlock-user-4.5-174; iSherlock 5.5: before iSherlock-user-5.5-174.	9.8	More Details
CVE-2022-46280	A use of uninitialized pointer vulnerability exists in the PQS format pFormat functionality of Open Babel 3.1.1 and master commit 530dbfa3. A specially crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2023-3638	In GeoVision GV-ADR2701 cameras, an attacker could edit the login response to access the web application.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3519	Unauthenticated remote code execution	9.8	More Details
CVE-2023-37289	It is identified a vulnerability of Unrestricted Upload of File with Dangerous Type in the file uploading function in InfoDoc Document On-line Submission and Approval System, which allows an unauthenticated remote attacker can exploit this vulnerability without logging system to upload and run arbitrary executable files to perform arbitrary system commands or disrupt service. This issue affects Document On-line Submission and Approval System: 22547, 22567.	9.8	More Details
CVE-2023-38408	The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.	9.8	More Details
CVE-2023-38203	Adobe ColdFusion versions 2018u17 (and earlier), 2021u7 (and earlier) and 2023u1 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction.	9.8	More Details
CVE-2023-37165	Millhouse-Project v1.414 was discovered to contain a remote code execution (RCE) vulnerability via the component /add_post_sql.php.	9.8	More Details
CVE-2023-31753	SQL injection vulnerability in diskusi.php in eNdonesia 8.7, allows an attacker to execute arbitrary SQL commands via the "rid=" parameter.	9.8	More Details
CVE-2023-38632	async-sockets-cpp through 0.3.1 has a stack-based buffer overflow in tcpsocket.hpp when processing malformed TCP packets.	9.8	More Details
CVE-2023-37677	Pligg CMS v2.0.2 (also known as Kliqqi) was discovered to contain a remote code execution (RCE) vulnerability in the component admin_editor.php.	9.8	More Details
CVE-2023-35087	It is identified a format string vulnerability in ASUS RT-AX56U V2 & RT-AC86U. This vulnerability is caused by lacking validation for a specific value when calling cm_processChangedConfigMsg in ccm_processREQ_CHANGED_CONFIG function in AiMesh system. An unauthenticated remote attacker can exploit this vulnerability without privilege to perform remote arbitrary code execution, arbitrary system operation or disrupt service. This issue affects RT-AX56U V2: 3.0.0.4.386_50460; RT-AC86U: 3.0.0.4_386_51529.	9.8	More Details
CVE-2023-38646	Metabase open source before 0.46.6.1 and Metabase Enterprise before 1.46.6.1 allow attackers to execute arbitrary commands on the server, at the server's privilege level. Authentication is not required for exploitation. The other fixed versions are 0.45.4.1, 1.45.4.1, 0.44.7.1, 1.44.7.1, 0.43.7.2, and 1.43.7.2.	9.8	More Details
CVE-2023-26301	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints.	9.8	More Details
CVE-2023-37903	vm2 is an open source vm/sandbox for Node.js. In vm2 for versions up to and including 3.9.19, Node.js custom inspect function allows attackers to escape the sandbox and run arbitrary code. This may result in Remote Code Execution, assuming the attacker has arbitrary code execution primitive inside the context of vm2 sandbox. There are no patches and no known workarounds. Users are advised to find an alternative software.	9.8	More Details
CVE-2022-41793	An out-of-bounds write vulnerability exists in the CSR format title functionality of Open Babel 3.1.1 and master commit 530dbfa3. A specially crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2022-42885	A use of uninitialized pointer vulnerability exists in the GRO format res functionality of Open Babel 3.1.1 and master commit 530dbfa3. A specially crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2022-43467	An out-of-bounds write vulnerability exists in the PQS format coord_file functionality of Open Babel 3.1.1 and master commit 530dbfa3. A specially crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2022-44451	A use of uninitialized pointer vulnerability exists in the MSI format atom functionality of Open Babel 3.1.1 and master commit 530dbfa3. A specially crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2023-37917	KubePi is an opensource kubernetes management panel. A normal user has permission to create/update users, they can become admin by editing the `isadmin` value in the request. As a result any user may take administrative control of KubePi. This issue has been addressed in version 1.6.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.1	More Details
CVE-2023-37471	Open Access Management (OpenAM) is an access management solution that includes Authentication, SSO, Authorization, Federation, Entitlements and Web Services Security. OpenAM up to version 14.7.2 does not properly validate the signature of SAML responses received as part of the SAMLv1.x Single Sign-On process. Attackers can use this fact to impersonate any OpenAM user, including the administrator, by sending a specially crafted SAML response to the SAMLPOSTProfileServlet servlet. This problem has been patched in OpenAM 14.7.3-SNAPSHOT and later. User unable to upgrade should comment servlet `SAMLPOSTProfileServlet` from their pom file. See the linked GHSA for details.	9.1	More Details
CVE-2023-34034	Using "**" as a pattern in Spring Security configuration for WebFlux creates a mismatch in pattern matching between Spring Security and Spring WebFlux, and the potential for a security bypass.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30799	MikroTik RouterOS stable before 6.49.7 and long-term through 6.48.6 are vulnerable to a privilege escalation issue. A remote and authenticated attacker can escalate privileges from admin to super-admin on the Winbox or HTTP interface. The attacker can abuse this vulnerability to execute arbitrary code on the system.	9.1	More Details
CVE-2023-32478	Dell PowerStore versions prior to 3.5.0.1 contain an insertion of sensitive information into log file vulnerability. A high privileged malicious user could potentially exploit this vulnerability, leading to sensitive information disclosure.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Refere
CVE-2023-22506	This High severity Injection and RCE (Remote Code Execution) vulnerability known as CVE-2023-22506 was introduced in version 8.0.0 of Bamboo Data Center. This Injection and RCE (Remote Code Execution) vulnerability, with a CVSS Score of 7.5, allows an authenticated attacker to modify the actions taken by a system call and execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction. Atlassian recommends that you upgrade your instance to latest version. If you're unable to upgrade to latest, upgrade to one of these fixed versions: 9.2.3 and 9.3.1. See the release notes ([https://confluence.atlassian.com/bambooreleases/bamboo-release-notes-1189793869.htmllhttps://confluence.atlassian.com/bambooreleases/bamboo-release-notes-1189793869.html]). You can download the latest version of Bamboo Data Center and Bamboo Server from the download center ([https://www.atlassian.com/software/bamboo/download-archiveslhttps://www.atlassian.com/software/bamboo/download-archives]). This vulnerability was reported via our Penetration Testing program.	8.8	More Details
CVE-2023-37258	DataEase is an open source data visualization analysis tool. Prior to version 1.18.9, DataEase has a SQL injection vulnerability that can bypass blacklists. The vulnerability has been fixed in v1.18.9. There are no known workarounds.	8.8	More Details
CVE-2023-31462	An issue was discovered in SteelSeries GG 36.0.0. An attacker can change values in an unencrypted database that is writable for all users on the computer, in order to trigger code execution with higher privileges.	8.8	More Details
CVE-2023-33876	A use-after-free vulnerability exists in the way Foxit Reader 12.1.2.15332 handles destroying annotations. Specially crafted Javascript code inside a malicious PDF document can trigger reuse of a previously freed object, which can lead to memory corruption and result in arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled.	8.8	More Details
CVE-2023-33866	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 12.1.2.15332. By prematurely deleting objects associated with pages, a specially crafted PDF document can trigger the reuse of previously freed memory, which can lead to arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled.	8.8	More Details
CVE-2023-32664	A type confusion vulnerability exists in the Javascript checkThisBox method as implemented in Foxit Reader 12.1.2.15332. Specially crafted Javascript code inside a malicious PDF document can cause memory corruption and lead to remote code execution. User would need to open a malicious file to trigger the vulnerability.	8.8	More Details
CVE-2023-28744	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 12.1.1.15289. A specially crafted PDF document can trigger the reuse of previously freed memory by manipulating form fields of a specific type. This can lead to memory corruption and arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled.	8.8	More Details
CVE-2023-27379	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 12.1.2.15332. By prematurely deleting objects associated with pages, a specially crafted PDF document can trigger the reuse of previously freed memory, which can lead to arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled.	8.8	More Details
CVE-2023-28754	Deserialization of Untrusted Data vulnerability in Apache ShardingSphere-Agent, which allows attackers to execute arbitrary code by constructing a special YAML configuration file. The attacker needs to have permission to modify the ShardingSphere Agent YAML configuration file on the target machine, and the target machine can access the URL with the arbitrary code JAR. An attacker can use SnakeYAML to deserialize java.net.URLClassLoader and make it load a JAR from a specified URL, and then deserialize javax.script.ScriptEngineManager to load code using that ClassLoader. When the ShardingSphere JVM process starts and uses the ShardingSphere-Agent, the arbitrary code specified by the attacker will be executed during the deserialization of the YAML configuration file by the Agent. This issue affects ShardingSphere-Agent: through 5.3.2. This vulnerability is fixed in Apache ShardingSphere 5.4.0.	8.8	More Details
CVE-2023-37650	A Cross-Site Request Forgery (CSRF) in the Admin portal of Cockpit CMS v2.5.2 allows attackers to execute arbitrary Administrator commands.	8.8	More Details
CVE-2023-26217	The Data Exchange Add-on component of TIBCO Software Inc.'s TIBCO EBX Add-ons contains an easily exploitable vulnerability that allows a low privileged user with import permissions and network access to the EBX server to execute arbitrary SQL statements on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO EBX Add-ons: versions 4.5.17 and below, versions 5.6.2 and below, version 6.1.0.	8.8	More Details
CVE-2022-30280	/SecurityManagement/html/createuser.jsf in Nokia NetAct 22 allows CSRF. A remote attacker is able to create users with arbitrary privileges, even administrative privileges. The application (even if it implements a CSRF token for the random GET request) does not ever verify a CSRF token. With a little help of social engineering/phishing (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.	8.8	More Details

CVE Number	Description	Base Score	Refere
CVE-2022-28864	An issue was discovered in Nokia NetAct 22 through the Administration of Measurements website section. A malicious user can edit or add the templateName parameter in order to include malicious code, which is then downloaded as a .csv or .xlsx file and executed on a victim machine. Here, the /aom/html/EditTemplate.jsf and /aom/html/ViewAllTemplatesPage.jsf templateName parameter is used.	8.8	More Details
CVE-2022-28863	An issue was discovered in Nokia NetAct 22. A remote user, authenticated to the website, can visit the Site Configuration Tool section and arbitrarily upload potentially dangerous files without restrictions via the /netact/sct dir parameter in conjunction with the operation=upload value.	8.8	More Details
CVE-2023-37291	Galaxy Software Services Vitals ESP is vulnerable to using a hard-coded encryption key. An unauthenticated remote attacker can generate a valid token parameter and exploit this vulnerability to access system to operate processes and access data. This issue affects Vitals ESP: from 3.0.8 through 6.2.0.	8.6	More Details
CVE-2023-34235	Strapi is an open-source headless content management system. Prior to version 4.10.8, it is possible to leak private fields if one is using the `t(number)` prefix. Knex query allows users to change the default prefix. For example, if someone changes the prefix to be the same as it was before or to another table they want to query, the query changes from `password` to `t1.password`. `password` is protected by filtering protections but `t1.password` is not protected. This can lead to filtering attacks on everything related to the object again, including admin passwords and reset-tokens. Version 4.10.8 fixes this issue.	8.6	More Details
CVE-2023-3722	An OS command injection vulnerability was found in the Avaya Aura Device Services Web application which could allow remote code execution as the Web server user via a malicious uploaded file. This issue affects Avaya Aura Device Services version 8.1.4.0 and earlier.	8.6	More Details
CVE-2023-35941	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.27.0, 1.26.4, 1.25.9, 1.24.10, and 1.23.12, a malicious client is able to construct credentials with permanent validity in some specific scenarios. This is caused by the some rare scenarios in which HMAC payload can be always valid in OAuth2 filter's check. Versions 1.27.0, 1.26.4, 1.25.9, 1.24.10, and 1.23.12 have a fix for this issue. As a workaround, avoid wildcards/prefix domain wildcards in the host's domain configuration.	8.6	More Details
CVE-2023-25837	There is a Cross-site Scripting vulnerability in Esri ArcGIS Enterprise Sites versions 10.8.1 – 10.9 that may allow a remote, authenticated attacker to create a crafted link which when clicked by a victim could potentially execute arbitrary JavaScript code in the target's browser. The privileges required to execute this attack are high. The impact to Confidentiality, Integrity and Availability are High.	8.4	More Details
CVE-2023-25835	There is a stored Cross-site Scripting vulnerability in Esri Portal for ArcGIS Enterprise Sites versions 10.8.1 – 11.1 that may allow a remote, authenticated attacker to create a crafted link that is stored in the site configuration which when clicked could potentially execute arbitrary JavaScript code in the victims browser. The privileges required to execute this attack are high. The impact to Confidentiality, Integrity and Availability are High.	8.4	More Details
CVE-2022-43910	IBM Security Guardium 11.3 could allow a local user to escalate their privileges due to improper permission controls. IBM X-Force ID: 240908.	8.4	More Details
CVE-2023-3466	Reflected Cross-Site Scripting (XSS)	8.3	More Details
CVE-2023-3548	An unauthorized user could gain account access to IQ Wifi 6 versions prior to 2.0.2 by conducting a brute force authentication attack.	8.3	More Details
CVE-2023-3486	An authentication bypass exists in PaperCut NG versions 22.0.12 and prior that could allow a remote, unauthenticated attacker to upload arbitrary files to the PaperCut NG host’s file storage. This could exhaust system resources and prevent the service from operating as expected.	8.2	More Details
CVE-2023-35944	Envoy is an open source edge and service proxy designed for cloud-native applications. Envoy allows mixed-case schemes in HTTP/2, however, some internal scheme checks are case-sensitive. Prior to versions 1.27.0, 1.26.4, 1.25.9, 1.24.10, and 1.23.12, this can lead to the rejection of requests with mixed-case schemes such as `htTp` or `htTps`, or the bypassing of some requests such as `https` in unencrypted connections. With a fix in versions 1.27.0, 1.26.4, 1.25.9, 1.24.10, and 1.23.12, Envoy will now lowercase scheme values by default, and change the internal scheme checks that were case-sensitive to be case-insensitive. There are no known workarounds for this issue.	8.2	More Details
CVE-2023-32258	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_LOGOFF and SMB2_CLOSE commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel.	8.1	More Details
CVE-2022-28733	Integer underflow in grub_net_recv_ip4_packets; A malicious crafted IP packet can lead to an integer underflow in grub_net_recv_ip4_packets() function on rsm->total_len value. Under certain circumstances the total_len value may end up wrapping around to a small integer number which will be used in memory allocation. If the attack succeeds in such way, subsequent operations can write past the end of the buffer.	8.1	More Details
CVE-2022-28734	Out-of-bounds write when handling split HTTP headers; When handling split HTTP headers, GRUB2 HTTP code accidentally moves its internal data buffer point by one position. This can lead to a out-of-bound write further when parsing the HTTP request, writing a NULL byte past the buffer. It's conceivable that an attacker controlled set of packets can lead to corruption of the GRUB2's internal memory metadata.	8.1	More Details
CVE-2023-32257	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_SESSION_SETUP and SMB2_LOGOFF commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel.	8.1	More Details
CVE-2022-43607	An out-of-bounds write vulnerability exists in the MOL2 format attribute and value functionality of Open Babel 3.1.1 and master commit 530dbfa3. A specially crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.1	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-34625	ShowMojo MojoBox Digital Lockbox 1.4 is vulnerable to Authentication Bypass. The implementation of the lock opening mechanism via Bluetooth Low Energy (BLE) is vulnerable to replay attacks. A malicious user is able to intercept BLE requests and replicate them to open the lock at any time. Alternatively, an attacker with physical access to the device on which the Android app is installed, can obtain the latest BLE messages via the app logs and use them for opening the lock.	8.1	More Details
CVE-2023-37460	Plexis Archiver is a collection of Plexus components to create archives or extract archives to a directory with a unified `Archiver`/`UnArchiver` API. Prior to version 4.8.0, using AbstractUnArchiver for extracting an archive might lead to an arbitrary file creation and possibly remote code execution. When extracting an archive with an entry that already exists in the destination directory as a symbolic link whose target does not exist - the `resolveFile()` function will return the symlink's source instead of its target, which will pass the verification that ensures the file will not be extracted outside of the destination directory. Later `Files.newOutputStream()`, that follows symlinks by default, will actually write the entry's content to the symlink's target. Whoever uses plexus archiver to extract an untrusted archive is vulnerable to an arbitrary file creation and possibly remote code execution. Version 4.8.0 contains a patch for this issue.	8.1	More Details
CVE-2023-3484	An issue has been discovered in GitLab EE affecting all versions starting from 12.8 before 15.11.11, all versions starting from 16.0 before 16.0.7, all versions starting from 16.1 before 16.1.2. An attacker could change the name or path of a public top-level group in certain situations.	8.0	More Details
CVE-2023-3467	Privilege Escalation to root administrator (nsroot)	8.0	More Details
CVE-2023-3842	A vulnerability was found in Pointware EasyInventory 1.0.12.0 and classified as critical. This issue affects some unknown processing of the file C:\Program Files (x86)\EasyInventory\Easy2W.exe. The manipulation leads to unquoted search path. Attacking locally is a requirement. The identifier VDB-235193 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.8	More Details
CVE-2023-34394	In Keysight Geolocation Server v2.4.2 and prior, an attacker could upload a specially crafted malicious file or delete any file or directory with SYSTEM privileges due to an improper path validation, which could result in local privilege escalation or a denial-of-service condition.	7.8	More Details
CVE-2023-28730	A memory corruption vulnerability Panasonic Control FPWIN Pro versions 7.6.0.3 and all previous versions may allow arbitrary code execution when opening specially crafted project files.	7.8	More Details
CVE-2023-36853	In Keysight Geolocation Server v2.4.2 and prior, a low privileged attacker could create a local ZIP file containing a malicious script in any location. The attacker could abuse this to load a DLL with SYSTEM privileges.	7.8	More Details
CVE-2023-28729	A type confusion vulnerability in Panasonic Control FPWIN Pro versions 7.6.0.3 and all previous versions may allow arbitrary code execution when opening specially crafted project files.	7.8	More Details
CVE-2023-28728	A stack-based buffer overflow in Panasonic Control FPWIN Pro versions 7.6.0.3 and all previous versions may allow arbitrary code execution when opening specially crafted project files.	7.8	More Details
CVE-2023-3776	A use-after-free vulnerability in the Linux kernel's net/sched: cls_fw component can be exploited to achieve local privilege escalation. If tcf_change_indev() fails, fw_set_parms() will immediately return an error after incrementing or decrementing the reference counter in tcf_bind_filter(). If an attacker can control the reference counter and set it to zero, they can cause the reference to be freed, leading to a use-after-free vulnerability. We recommend upgrading past commit 0323bce598eea038714f941ce2b22541c46d488f.	7.8	More Details
CVE-2021-39822	Adobe InDesign versions 16.3 (and earlier), and 16.3.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious BMP file.	7.8	More Details
CVE-2023-3812	An out-of-bounds memory access flaw was found in the Linux kernel’s TUN/TAP device driver functionality in how a user generates a malicious (too big) networking packet when napi frags is enabled. This flaw allows a local user to crash or potentially escalate their privileges on the system.	7.8	More Details
CVE-2023-26077	Atera Agent through 1.8.3.6 on Windows Creates a Temporary File in a Directory with Insecure Permissions.	7.8	More Details
CVE-2023-3609	A use-after-free vulnerability in the Linux kernel's net/sched: cls_u32 component can be exploited to achieve local privilege escalation. If tcf_change_indev() fails, u32_set_parms() will immediately return an error after incrementing or decrementing the reference counter in tcf_bind_filter(). If an attacker can control the reference counter and set it to zero, they can cause the reference to be freed, leading to a use-after-free vulnerability. We recommend upgrading past commit 04c55383fa5689357bcdd2c8036725a55ed632bc.	7.8	More Details
CVE-2023-3610	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. Flaw in the error handling of bound chains causes a use-after-free in the abort path of NFT_MSG_NEWRULE. The vulnerability requires CAP_NET_ADMIN to be triggered. We recommend upgrading past commit 4bedf9eee016286c835e3d8fa981ddece5338795.	7.8	More Details
CVE-2023-26078	Privilege escalation vulnerability was discovered in Atera Agent 1.8.4.4 and prior on Windows due to mishandling of privileged APIs.	7.8	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-3611	An out-of-bounds write vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege escalation. The qfq_change_agg() function in net/sched/sch_qfq.c allows an out-of-bounds write because lmax is updated according to packet sizes without bounds checks. We recommend upgrading past commit 3e337087c3b5805fe0b8a46ba622a962880b5d64.	7.8	More Details
CVE-2023-28133	Local privilege escalation in Check Point Endpoint Security Client (version E87.30) via crafted OpenSSL configuration file	7.8	More Details
CVE-2023-36826	Sentry is an error tracking and performance monitoring platform. Starting in version 8.21.0 and prior to version 23.5.2, an authenticated user can download a debug or artifact bundle from arbitrary organizations and projects with a known bundle ID. The user does not need to be a member of the organization or have permissions on the project. A patch was issued in version 23.5.2 to ensure authorization checks are properly scoped on requests to retrieve debug or artifact bundles. Authenticated users who do not have the necessary permissions on the particular project are no longer able to download them. Sentry SaaS users do not need to take any action. Self-Hosted Sentry users should upgrade to version 23.5.2 or higher.	7.7	More Details
CVE-2023-22428	Improper privilege validation in Command Centre Server allows authenticated operators to modify Division lineage. This issue affects Command Centre: vEL8.80 prior to vEL8.80.1192 (MR2), vEL8.70 prior to vEL8.70.2185 (MR4), vEL8.60 prior to vEL8.60.2347 (MR6), vEL8.50 prior to vEL8.50.2831(MR8), vEL8.40 and prior.	7.6	More Details
CVE-2023-37899	Feathersjs is a framework for creating web APIs and real-time applications with TypeScript or JavaScript. Feathers socket handler did not catch invalid string conversion errors like `const message = ${{ toString: '' }}` which would cause the NodeJS process to crash when sending an unexpected Socket.io message like `socket.emit('find', { toString: '' })`. A fix has been released in versions 5.0.8 and 4.5.18. Users are advised to upgrade. There is no known workaround for this vulnerability.	7.5	More Details
CVE-2023-31461	Attackers can exploit an open API listener on SteelSeries GG 36.0.0 to create a sub-application that will be executed automatically from a controlled location, because of a path traversal vulnerability.	7.5	More Details
CVE-2022-31457	RTX TRAP v1.0 allows attackers to perform a directory traversal via a crafted request sent to the endpoint /data/.	7.5	More Details
CVE-2023-36339	An access control issue in WebBoss.io CMS v3.7.0.1 allows attackers to access the Website Backup Tool via a crafted GET request.	7.5	More Details
CVE-2023-34966	An infinite loop vulnerability was found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets sent by the client, the core unmarshalling function sl_unpack_loop() did not validate a field in the network packet that contains the count of elements in an array-like structure. By passing 0 as the count value, the attacked function will run in an endless loop consuming 100% CPU. This flaw allows an attacker to issue a malformed RPC request, triggering an infinite loop, resulting in a denial of service condition.	7.5	More Details
CVE-2023-35067	Plaintext Storage of a Password vulnerability in Infodrom Software E-Invoice Approval System allows Read Sensitive Strings Within an Executable.This issue affects E-Invoice Approval System: before v.20230701.	7.5	More Details
CVE-2023-3417	Thunderbird allowed the Text Direction Override Unicode Character in filenames. An email attachment could be incorrectly shown as being a document file, while in fact it was an executable file. Newer versions of Thunderbird will strip the character and show the correct file extension. This vulnerability affects Thunderbird < 115.0.1 and Thunderbird < 102.13.1.	7.5	More Details
CVE-2023-38493	Armeria is a microservice framework Spring supports Matrix variables. When Spring integration is used, Armeria calls Spring controllers via `TomcatService` or `JettyService` with the path that may contain matrix variables. Prior to version 1.24.3, the Armeria decorators might not invoked because of the matrix variables. If an attacker sends a specially crafted request, the request may bypass the authorizer. Version 1.24.3 contains a patch for this issue.	7.5	More Details
CVE-2023-35077	An out-of-bounds write vulnerability on windows operating systems causes the Ivanti AntiVirus Product to crash. Update to Ivanti AV Product version 7.9.1.285 or above.	7.5	More Details
CVE-2023-25838	There is SQL injection vulnerability in Esri ArcGIS Insights 2022.1 for ArcGIS Enterprise and that may allow a remote, authorized attacker to execute arbitrary SQL commands against the back-end database. The effort required to generate the crafted input required to exploit this issue is complex and requires significant effort before a successful attack can be expected.	7.5	More Details
CVE-2023-32247	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the handling of SMB2_SESSION_SETUP commands. The issue results from the lack of control of resource consumption. An attacker can leverage this vulnerability to create a denial-of-service condition on the system.	7.5	More Details
CVE-2023-37915	OpenDDS is an open source C++ implementation of the Object Management Group (OMG) Data Distribution Service (DDS). OpenDDS crashes while parsing a malformed `PID_PROPERTY_LIST` in a DATA submessage during participant discovery. Attackers can remotely crash OpenDDS processes by sending a DATA submessage containing the malformed parameter to the known multicast port. This issue has been addressed in version 3.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2022-46902	An issue was discovered in Vocera Report Server and Voice Server 5.x through 5.8. There is a Path Traversal for an Unzip operation. The Vocera Report Console contains a websocket function that allows for the restoration of the database from a ZIP archive that expects a SQL import file. During the unzip operation, the code takes file paths from the ZIP archive and writes them to a Vocera temporary directory. Unfortunately, the code does not properly check if the file paths include directory traversal payloads that would escape the intended destination.	7.5	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-37649	Incorrect access control in the component /models/Content of Cockpit CMS v2.5.2 allows unauthorized attackers to access sensitive data.	7.5	More Details
CVE-2023-32248	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the handling of SMB2_TREE_CONNECT and SMB2_QUERY_INFO commands. The issue results from the lack of proper validation of a pointer prior to accessing it. An attacker can leverage this vulnerability to create a denial-of-service condition on the system.	7.5	More Details
CVE-2023-37601	Office Suite Premium v10.9.1.42602 was discovered to contain a local file inclusion (LFI) vulnerability via the component /etc/hosts.	7.5	More Details
CVE-2023-32252	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the handling of SMB2_LOGOFF commands. The issue results from the lack of proper validation of a pointer prior to accessing it. An attacker can leverage this vulnerability to create a denial-of-service condition on the system.	7.5	More Details
CVE-2023-34434	Deserialization of Untrusted Data Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.7.0. The attacker could bypass the current logic and achieve arbitrary file reading. To solve it, users are advised to upgrade to Apache InLong's 1.8.0 or cherry-pick https://github.com/apache/inlong/pull/8130 .	7.5	More Details
CVE-2023-37920	Certifi is a curated collection of Root Certificates for validating the trustworthiness of SSL certificates while verifying the identity of TLS hosts. Certifi prior to version 2023.07.22 recognizes "e-Tugra" root certificates. e-Tugra's root certificates were subject to an investigation prompted by reporting of security issues in their systems. Certifi 2023.07.22 removes root certificates from "e-Tugra" from the root store.	7.5	More Details
CVE-2023-37290	InfoDoc Document On-line Submission and Approval System lacks sufficient restrictions on the available tags within its HTML to PDF conversion function, and allowing an unauthenticated attackers to load remote or local resources through HTML tags such as iframe. This vulnerability allows unauthenticated remote attackers to perform Server-Side Request Forgery (SSRF) attacks, gaining unauthorized access to arbitrary system files and uncovering the internal network topology.	7.5	More Details
CVE-2022-46899	An issue was discovered in Vocera Report Server and Voice Server 5.x through 5.8. There is Arbitrary File Upload. The BaseController class, that each of the service controllers derives from, allows for the upload of arbitrary files. If the HTTP request is a multipart/form-data POST request, any parameters with a filename entry will have their content written to a file in the Vocera upload-staging directory with the specified filename in the parameter.	7.5	More Details
CVE-2023-2626	There exists an authentication bypass vulnerability in OpenThread border router devices and implementations. This issue allows unauthenticated nodes to craft radio frames using “Key ID Mode 2”: a special mode using a static encryption key to bypass security checks, resulting in arbitrary IP packets being allowed on the Thread network. This provides a pathway for an attacker to send/receive arbitrary IPv6 packets to devices on the LAN, potentially exploiting them if they lack additional authentication or contain any network vulnerabilities that would normally be mitigated by the home router’s NAT firewall. Effected devices have been mitigated through an automatic update beyond the affected range.	7.5	More Details
CVE-2023-34429	Weintek Weincloud v0.13.6 could allow an attacker to cause a denial-of-service condition for Weincloud by sending a forged JWT token.	7.5	More Details
CVE-2022-46901	An issue was discovered in Vocera Report Server and Voice Server 5.x through 5.8. There is an Access Control Violation for Database Operations. The Vocera Report Console contains a websocket interface that allows for the unauthenticated execution of various tasks and database functions. This includes system tasks, and backing up, loading, and clearing of the database.	7.5	More Details
CVE-2023-3813	The Jupiter X Core plugin for WordPress is vulnerable to arbitrary file downloads in versions up to, and including, 2.5.0. This makes it possible for unauthenticated attackers to download the contents of arbitrary files on the server, which can contain sensitive information. The requires the premium version of the plugin to be activated.	7.5	More Details
CVE-2023-30200	In the module “Image: WebP, Compress, Zoom, Lazy load, Alt & More” (ultimateimagetool) in versions up to 2.1.02 from Advanced Plugins for PrestaShop, a guest can download personal informations without restriction by performing a path traversal attack.	7.5	More Details
CVE-2023-38200	A flaw was found in Keylime. Due to their blocking nature, the Keylime registrar is subject to a remote denial of service against its SSL connections. This flaw allows an attacker to exhaust all available connections.	7.5	More Details
CVE-2023-35134	Weintek Weincloud v0.13.6 could allow an attacker to reset a password with the corresponding account’s JWT token only.	7.4	More Details
CVE-2023-3873	A vulnerability, which was classified as critical, has been found in Campcodes Beauty Salon Management System 1.0. This issue affects some unknown processing of the file /admin/index.php. The manipulation of the argument username leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235235.	7.3	More Details
CVE-2022-37331	An out-of-bounds write vulnerability exists in the Gaussian format orientation functionality of Open Babel 3.1.1 and master commit 530dbfa3. A specially crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.3	More Details
CVE-2023-3805	A vulnerability, which was classified as critical, has been found in Xiamen Four Letter Video Surveillance Management System up to 20230712. This issue affects some unknown processing in the library UserInfoAction.class of the component Login. The manipulation leads to improper authorization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-235073 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details

CVE Number	Description	Base Score	Refere
CVE-2021-35391	Server Side Request Forgery vulnerability found in Deskpro Support Desk v2021.21.6 allows attackers to execute arbitrary code via a crafted URL.	7.2	More Details
CVE-2023-2761	The User Activity Log WordPress plugin before 1.6.3 does not properly sanitise and escape the `txtsearch` parameter before using it in a SQL statement in some admin pages, leading to a SQL injection exploitable by high privilege users such as admin.	7.2	More Details
CVE-2023-35086	It is identified a format string vulnerability in ASUS RT-AX56U V2 & RT-AC86U. This vulnerability is caused by directly using input as a format string when calling syslog in logmessage_normal function, in the do_detwan_cgi module of httpd. A remote attacker with administrator privilege can exploit this vulnerability to perform remote arbitrary code execution, arbitrary system operation or disrupt service. This issue affects RT-AX56U V2: 3.0.0.4.386_50460; RT-AC86U: 3.0.0.4_386_51529.	7.2	More Details
CVE-2023-3820	SQL Injection in GitHub repository pimcore/pimcore prior to 10.6.4.	7.2	More Details
CVE-2023-37362	Weintek Weincloud v0.13.6 could allow an attacker to abuse the registration functionality to login with testing credentials to the official website.	7.2	More Details
CVE-2023-38056	Improper Neutralization of commands allowed to be executed via OTRS System Configuration e.g. SchedulerCronTaskModule using UnitTests modules allows any authenticated attacker with admin privileges local execution of Code.This issue affects OTRS: from 7.0.X before 7.0.45, from 8.0.X before 8.0.35; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34.	7.2	More Details
CVE-2023-36502	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ctthemes Balkon plugin <= 1.3.2 versions.	7.1	More Details
CVE-2023-33925	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in PluginForage WooCommerce Product Categories Selection Widget plugin <= 2.0 versions.	7.1	More Details
CVE-2023-34017	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in FiveStarPlugins Five Star Restaurant Reservations plugin <= 2.6.7 versions.	7.1	More Details
CVE-2023-21406	Ariel Harush and Roy Hodir from OTORIO have found a flaw in the AXIS A1001 when communicating over OSDP. A heap-based buffer overflow was found in the pacsiod process which is handling the OSDP communication allowing to write outside of the allocated buffer. By appending invalid data to an OSDP message it was possible to write data beyond the heap allocated buffer. The data written outside the buffer could be used to execute arbitrary code. lease refer to the Axis security advisory for more information, mitigation and affected products and software versions.	7.1	More Details
CVE-2023-36385	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in wpxpo PostX – Gutenberg Post Grid Blocks plugin <= 2.9.9 versions.	7.1	More Details
CVE-2023-32265	A potential security vulnerability has been identified in the Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server, Enterprise Developer, Visual COBOL, and COBOL Server. An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the hardening guide in the product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue. Given the right conditions this vulnerability could be exploited to expose a service account password. The account corresponding to the exposed credentials usually has limited privileges and, in many cases would only be useful for extracting details of other user accounts and similar information.	7.1	More Details
CVE-2023-25074	Improper privilege validation in Command Centre Server allows authenticated unprivileged operators to modify and view Competencies. This issue affects Command Centre: vEL8.90 prior to vEL8.90.1318 (MR1), vEL8.80 prior to vEL8.80.1192 (MR2), vEL8.70 prior to vEL8.70.2185 (MR4), vEL8.60 prior to vEL8.60.2347 (MR6), vEL8.50 prior to vEL8.50.2831 (MR8), all versions vEL8.40 and prior.	7.1	More Details
CVE-2023-3567	A use-after-free flaw was found in vcs_read in drivers/tty/vt/vc_screen.c in vc_screen in the Linux Kernel. This issue may allow an attacker with local user access to cause a system crash or leak internal kernel information.	7.1	More Details
CVE-2023-35043	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Neha Goel Recent Posts Slider plugin <= 1.1 versions.	7.1	More Details
CVE-2023-36501	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Michael Winkler teachPress plugin <= 9.0.2 versions.	7.1	More Details
CVE-2023-3321	A vulnerability exists by allowing low-privileged users to read and update the data in various directories used by the Zenon system. An attacker could exploit the vulnerability by using specially crafted programs to exploit the vulnerabilities by allowing them to run on the zenon installed hosts. This issue affects ABB Ability™ zenon: from 11 build through 11 build 106404.	7.0	More Details
CVE-2023-3322	A vulnerability exists by allowing low-privileged users to read and update the data in various directories used by the Zenon system. An attacker could exploit the vulnerability by using specially crafted programs to exploit the vulnerabilities by allowing them to run on the zenon installed hosts. This issue affects ABB Ability™ zenon: from 11 build through 11 build 106404.	7.0	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-37907	Cryptomator is data encryption software for users who store their files in the cloud. Prior to version 1.9.2, the MSI installer provided on the homepage allows local privilege escalation (LPE) for low privileged users, if already installed. The problem occurs as the repair function of the MSI spawns two administrative CMDs. A simple LPE is possible via a breakout. Version 1.9.2 fixes this issue.	7.0	More Details
CVE-2023-3640	A possible unauthorized memory access flaw was found in the Linux kernel's cpu_entry_area mapping of X86 CPU data to memory, where a user may guess the location of exception stacks or other important data. Based on the previous CVE-2023-0597, the 'Randomize per-cpu entry area' feature was implemented in /arch/x86/mm/cpu_entry_area.c, which works through the init_cea_offsets() function when KASLR is enabled. However, despite this feature, there is still a risk of per-cpu entry area leaks. This issue could allow a local user to gain access to some important data with memory in an expected location and potentially escalate their privileges on the system.	7.0	More Details
CVE-2023-25839	There is SQL injection vulnerability in Esri ArcGIS Insights Desktop for Mac and Windows version 2022.1 that may allow a local, authorized attacker to execute arbitrary SQL commands against the back-end database. The effort required to generate the crafted input required to exploit this issue is complex and requires significant effort before a successful attack can be expected.	7.0	More Details
CVE-2023-37918	Dapr is a portable, event-driven, runtime for building distributed applications across cloud and edge. A vulnerability has been found in Dapr that allows bypassing API token authentication, which is used by the Dapr sidecar to authenticate calls coming from the application, with a well-crafted HTTP request. Users who leverage API token authentication are encouraged to upgrade Dapr to 1.10.9 or to 1.11.2. This vulnerability impacts Dapr users who have configured API token authentication. An attacker could craft a request that is always allowed by the Dapr sidecar over HTTP, even if the `dapr-api-token` in the request is invalid or missing. The issue has been fixed in Dapr 1.10.9 or to 1.11.2. There are no known workarounds for this vulnerability.	6.8	More Details
CVE-2023-33951	A race condition vulnerability was found in the vmwgfx driver in the Linux kernel. The flaw exists within the handling of GEM objects. The issue results from improper locking when performing operations on an object. This flaw allows a local privileged user to disclose information in the context of the kernel.	6.7	More Details
CVE-2022-28735	The GRUB2's shim_lock verifier allows non-kernel files to be loaded on shim-powered secure boot systems. Allowing such files to be loaded may lead to unverified code and modules to be loaded in GRUB2 breaking the secure boot trust-chain.	6.7	More Details
CVE-2023-33952	A double-free vulnerability was found in handling vmw_buffer_object objects in the vmwgfx driver in the Linux kernel. This issue occurs due to the lack of validating the existence of an object prior to performing further free operations on the object, which may allow a local privileged user to escalate privileges and execute code in the context of the kernel.	6.7	More Details
CVE-2023-3463	All versions of GE Digital CIMPLICITY that are not adhering to SDG guidance and accepting documents from untrusted sources are vulnerable to memory corruption issues due to insufficient input validation, including issues such as out-of-bounds reads and writes, use-after-free, stack-based buffer overflows, uninitialized pointers, and a heap-based buffer overflow. Successful exploitation could allow an attacker to execute arbitrary code.	6.6	More Details
CVE-2023-37919	Cal.com is open-source scheduling software. A vulnerability allows active sessions associated with an account to remain active even after enabling 2FA. When activating 2FA on a Cal.com account that is logged in on two or more devices, the account stays logged in on the other device(s) stays logged in without having to verify the account owner's identity. As of time of publication, no known patches or workarounds exist.	6.5	More Details
CVE-2023-36503	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Max Foundry WordPress Button Plugin MaxButtons plugin <= 9.5.3 versions.	6.5	More Details
CVE-2023-29260	IBM Sterling Connect:Express for UNIX 1.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 252135.	6.5	More Details
CVE-2023-3750	A flaw was found in libvirt. The virStoragePoolObjListSearch function does not return a locked pool as expected, resulting in a race condition and denial of service when attempting to lock the same object from another thread. This issue could allow clients connecting to the read-only socket to crash the libvirt daemon.	6.5	More Details
CVE-2023-35942	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.27.0, 1.26.4, 1.25.9, 1.24.10, and 1.23.12, gRPC access loggers using listener's global scope can cause a `use-after-free` crash when the listener is drained. Versions 1.27.0, 1.26.4, 1.25.9, 1.24.10, and 1.23.12 have a fix for this issue. As a workaround, disable gRPC access log or stop listener update.	6.5	More Details
CVE-2023-3819	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository pimcore/pimcore prior to 10.6.4.	6.5	More Details
CVE-2022-46900	An issue was discovered in Vocera Report Server and Voice Server 5.x through 5.8. There is Path Traversal in the Task Exec filename. The Vocera Report Console contains various jobs that are executed on the server at specified intervals, e.g., backup, etc. An authenticated user has the ability to modify these entries and set the executable path and parameters.	6.5	More Details
CVE-2022-28737	There's a possible overflow in handle_image() when shim tries to load and execute crafted EFI executables; The handle_image() function takes into account the SizeOfRawData field from each section to be loaded. An attacker can leverage this to perform out-of-bound writes into memory. Arbitrary code execution is not discarded in such scenario.	6.5	More Details
CVE-2023-23833	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Steven Henty Drop Shadow Boxes plugin <= 1.7.10 versions.	6.5	More Details
CVE-2020-24275	A HTTP response header injection vulnerability in Swoole v4.5.2 allows attackers to execute arbitrary code via supplying a crafted URL.	6.5	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-38187	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	6.5	More Details
CVE-2023-34189	Exposure of Resource to Wrong Sphere Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.7.0. The attacker could use general users to delete and update the process, which only the admin can operate occurrences. Users are advised to upgrade to Apache InLong's 1.8.0 or cherry-pick https://github.com/apache/inlong/pull/8109 to solve it.	6.5	More Details
CVE-2023-26023	Planning Analytics Cartridge for Cloud Pak for Data 4.0 exposes sensitive information in logs which could lead an attacker to exploit this vulnerability to conduct further attacks. IBM X-Force ID: 247896.	6.5	More Details
CVE-2023-37916	KubePi is an opensource kubernetes management panel. The endpoint /kubepi/api/v1/users/search?pageNum=1&&pageSize=10 leak password hash of any user (including admin). A sufficiently motivated attacker may be able to crack leaded password hashes. This issue has been addressed in version 1.6.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2023-30433	IBM Security Verify Access 10.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 252186.	6.5	More Details
CVE-2023-38502	TDengine is an open source, time-series database optimized for Internet of Things devices. Prior to version 3.0.7.1, TDengine DataBase crashes on UDF nested query. This issue affects TDengine Databases which let users connect and run arbitrary queries. Version 3.0.7.1 has a patch for this issue.	6.5	More Details
CVE-2023-22363	A stack-based buffer overflow in the Command Centre Server allows an attacker to cause a denial of service attack via assigning cardholders to an Access Group. This issue affects Command Centre: vEL8.80 prior to vEL8.80.1192 (MR2)	6.5	More Details
CVE-2023-21405	Knud from Fraktal.fi has found a flaw in some Axis Network Door Controllers and Axis Network Intercoms when communicating over OSDP, highlighting that the OSDP message parser crashes the pacsiod process, causing a temporary unavailability of the door-controlling functionalities meaning that doors cannot be opened or closed. No sensitive or customer data can be extracted as the Axis device is not further compromised. Please refer to the Axis security advisory for more information, mitigation and affected products and software versions.	6.5	More Details
CVE-2023-38334	Omnis Studio 10.22.00 has incorrect access control. It advertises an irreversible feature for locking classes within Omnis libraries: it should be no longer possible to delete, view, change, copy, rename, duplicate, or print a locked class. Due to implementation issues, locked classes in Omnis libraries can be unlocked, and thus further analyzed and modified by Omnis Studio. This allows for further analyzing and also deleting, viewing, changing, copying, renaming, duplicating, or printing previously locked Omnis classes. This violates the expected behavior of an "irreversible operation."	6.5	More Details
CVE-2023-36806	Contao is an open source content management system. Starting in version 4.0.0 and prior to versions 4.9.42, 4.13.28, and 5.1.10, it is possible for untrusted backend users to inject malicious code into headline fields in the back end, which will be executed both in the element preview (back end) and on the website (front end). Installations are only affected if there are untrusted back end users who have the rights to modify headline fields, or other fields using the input unit widget. Contao 4.9.42, 4.13.28, and 5.1.10 have a patch for this issue. As a workaround, disable the login for all untrusted back end users.	6.5	More Details
CVE-2023-32476	Dell Hybrid Client version 2.0 contains a Sensitive Data Exposure vulnerability. An unauthenticated malicious user on the device can access hard coded secrets in javascript files.	6.4	More Details
CVE-2022-28736	There's a use-after-free vulnerability in grub_cmd_chainloader() function; The chainloader command is used to boot up operating systems that doesn't support multiboot and do not have direct support from GRUB2. When executing chainloader more than once a use-after-free vulnerability is triggered. If an attacker can control the GRUB2's memory allocation pattern sensitive data may be exposed and arbitrary code execution can be achieved.	6.4	More Details
CVE-2023-3863	A use-after-free flaw was found in nfc_llcp_find_local in net/nfc/llcp_core.c in NFC in the Linux kernel. This flaw allows a local user with special privileges to impact a kernel information leak issue.	6.4	More Details
CVE-2023-3850	A vulnerability has been found in SourceCodester Lost and Found Information System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /classes/Master.php?f=delete_category of the component HTTP POST Request Handler. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The identifier VDB-235201 was assigned to this vulnerability.	6.3	More Details
CVE-2023-3854	A vulnerability classified as critical has been found in phpscriptpoint BloodBank 1.1. Affected is an unknown function of the file /search of the component POST Parameter Handler. The manipulation of the argument country/city/blood_group_id leads to sql injection. It is possible to launch the attack remotely. VDB-235206 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3859	A vulnerability was found in phpscriptpoint Car Listing 1.6 and classified as critical. This issue affects some unknown processing of the file /search.php of the component GET Parameter Handler. The manipulation of the argument brand_id/model_id/car_condition/car_category_id/body_type_id/fuel_type_id/transmission_type_id/year/mileage_start/mileage_end/country/state/city leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-235211. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-3751	A vulnerability was found in Super Store Finder 3.6. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /index.php of the component POST Parameter Handler. The manipulation of the argument products leads to sql injection. The attack can be launched remotely. The identifier VDB-234421 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-38501	copyparty is file server software. Prior to version 1.8.7, the application contains a reflected cross-site scripting via URL-parameter `?k304=...` and `?setck=...`. The worst-case outcome of this is being able to move or delete existing files on the server, or upload new files, using the account of the person who clicks the malicious link. It is recommended to change the passwords of one's copyparty accounts, unless one have inspected one's logs and found no trace of attacks. Version 1.8.7 contains a patch for the issue.	6.3	More Details
CVE-2023-3836	A vulnerability classified as critical was found in Dahua Smart Park Management up to 20230713. This vulnerability affects unknown code of the file /emap/devicePoint_addImgIco?hasSubsystem=true. The manipulation of the argument upload leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-235162 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-38060	Improper Input Validation vulnerability in the ContentType parameter for attachments on TicketCreate or TicketUpdate operations of the OTRS Generic Interface modules allows any authenticated attacker to to perform an host header injection for the ContentType header of the attachment. This issue affects OTRS: from 7.0.X before 7.0.45, from 8.0.X before 8.0.35; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34.	6.3	More Details
CVE-2023-3826	A vulnerability has been found in IBOS OA 4.5.5 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /?r=recruit/resume/edit&op=status of the component Interview Handler. The manipulation of the argument resumeid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235147. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3324	A vulnerability exists by allowing low-privileged users to read and update the data in various directories used by the Zenon system. An attacker could exploit the vulnerability by using specially crafted programs to exploit the vulnerabilities by allowing them to run on the zenon installed hosts. This issue affects ABB Ability™ zenon: from 11 build through 11 build 106404.	6.3	More Details
CVE-2023-3811	A vulnerability was found in Hospital Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file patientprofile.php. The manipulation of the argument address leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235079.	6.3	More Details
CVE-2023-3799	A vulnerability was found in IBOS OA 4.5.5 and classified as critical. This issue affects some unknown processing of the file ?r=article/category/del of the component Delete Category Handler. The manipulation leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235067. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-35943	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.27.0, 1.26.4, 1.25.9, 1.24.10, and 1.23.12, the CORS filter will segfault and crash Envoy when the `origin` header is removed and deleted between `decodeHeaders`and `encodeHeaders`. Versions 1.27.0, 1.26.4, 1.25.9, 1.24.10, and 1.23.12 have a fix for this issue. As a workaround, do not remove the `origin` header in the Envoy configuration.	6.3	More Details
CVE-2023-3882	A vulnerability, which was classified as critical, has been found in Campcodes Beauty Salon Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/edit-accepted-appointment.php. The manipulation of the argument contactno leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-235244.	6.3	More Details
CVE-2023-3881	A vulnerability classified as critical was found in Campcodes Beauty Salon Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/forgot-password.php. The manipulation of the argument contactno leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235243.	6.3	More Details
CVE-2023-3880	A vulnerability classified as critical has been found in Campcodes Beauty Salon Management System 1.0. Affected is an unknown function of the file /admin/del_service.php. The manipulation of the argument editid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-235242 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-3879	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/del_category.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-235241 was assigned to this vulnerability.	6.3	More Details
CVE-2023-38745	Pandoc before 3.1.6 allows arbitrary file write: this can be triggered by providing a crafted image element in the input when generating files via the --extract-media option or outputting to PDF format. This allows an attacker to create or overwrite arbitrary files, depending on the privileges of the process running Pandoc. It only affects systems that pass untrusted user input to Pandoc and allow Pandoc to be used to produce a PDF or with the --extract-media option. NOTE: this issue exists because of an incomplete fix for CVE-2023-35936 (failure to properly account for double encoded path names).	6.3	More Details
CVE-2023-3878	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/about-us.php. The manipulation of the argument pagedes leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-235240.	6.3	More Details
CVE-2023-3877	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/add-services.php. The manipulation of the argument cost 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 vulnerability is VDB-235239.	6.3	More Details
CVE-2023-3876	A vulnerability was found in Campcodes Beauty Salon Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/search-appointment.php. The manipulation of the argument searchdata leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-235238 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-3810	A vulnerability was found in Hospital Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file patientappointment.php. The manipulation of the argument loginid/password/mobileno/appointmentdate/appointmenttime/patiente/dob/doct/city leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-235078 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-3874	A vulnerability, which was classified as critical, was found in Campcodes Beauty Salon Management System 1.0. Affected is an unknown function of the file /admin/admin-profile.php. The manipulation of the argument adminname leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-235236.	6.3	More Details
CVE-2023-3872	A vulnerability classified as critical was found in Campcodes Beauty Salon Management System 1.0. This vulnerability affects unknown code of the file /admin/edit-services.php. The manipulation of the argument editid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-235234 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-3871	A vulnerability classified as critical has been found in Campcodes Beauty Salon Management System 1.0. This affects an unknown part of the file /admin/edit_category.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-235233 was assigned to this vulnerability.	6.3	More Details
CVE-2023-3875	A vulnerability has been found in Campcodes Beauty Salon Management System 0.1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/del_feedback.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-235237 was assigned to this vulnerability.	6.3	More Details
CVE-2023-3791	A vulnerability was found in IBOS OA 4.5.5 and classified as critical. Affected by this issue is the function actionExport of the file ?r=contact/default/export of the component Personal Office Address Book. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-235058 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3809	A vulnerability was found in Hospital Management System 1.0. It has been classified as critical. This affects an unknown part of the file patient.php. The manipulation of the argument address leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-235077 was assigned to this vulnerability.	6.3	More Details
CVE-2023-3759	A vulnerability, which was classified as critical, was found in Intergard SGS 8.7.0. Affected is an unknown function. The manipulation leads to permission issues. 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-234444. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3808	A vulnerability was found in Hospital Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file patientforgotpassword.php. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-235076.	6.3	More Details
CVE-2023-3807	A vulnerability has been found in Campcodes Beauty Salon Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file edit_product.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235075.	6.3	More Details
CVE-2023-3806	A vulnerability, which was classified as critical, was found in SourceCodester House Rental and Property Listing System 1.0. Affected is an unknown function of the file btn_functions.php. The manipulation 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-235074 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-33832	IBM Spectrum Protect 8.1.0.0 through 8.1.17.0 could allow a local user to cause a denial of service due to due to improper time-of-check to time-of-use functionality. IBM X-Force ID: 256012.	6.2	More Details
CVE-2023-37164	Diafan CMS v6.0 was discovered to contain a reflected cross-site scripting via the cat_id parameter at /shop/?module=shop&action=search.	6.1	More Details
CVE-2023-38435	An improper neutralization of input during web page generation ('Cross-site Scripting') [CWE-79] vulnerability in Apache Felix Healthcheck Webconsole Plugin version 2.0.2 and prior may allow an attacker to perform a reflected cross-site scripting (XSS) attack. Upgrade to Apache Felix Healthcheck Webconsole Plugin 2.1.0 or higher.	6.1	More Details
CVE-2023-37733	An arbitrary file upload vulnerability in tduck-platform v4.0 allows attackers to execute arbitrary code via a crafted HTML file.	6.1	More Details
CVE-2023-2309	The wpForo Forum WordPress plugin before 2.1.9 does not escape some request parameters while in debug mode, leading to a Reflected Cross-Site Scripting vulnerability.	6.1	More Details
CVE-2023-3822	Cross-site Scripting (XSS) - Reflected in GitHub repository pimcore/pimcore prior to 10.6.4.	6.1	More Details
CVE-2023-37742	WebBoss.io CMS before v3.7.0.1 was discovered to contain a reflected cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2023-37728	IceWarp v10.2.1 was discovered to contain cross-site scripting (XSS) vulnerability via the color parameter.	6.1	More Details

CVE Number	Description	Base Score	Refere
CVE-2021-39421	A cross-site scripting (XSS) vulnerability in SeedDMS v6.0.15 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2023-37613	A cross-site scripting (XSS) vulnerability in Assembly Software Trialworks v11.4 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the asset src parameter.	6.1	More Details
CVE-2023-37600	Office Suite Premium Version v10.9.1.42602 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the id parameter at /api?path=profile.	6.1	More Details
CVE-2022-31458	RTX TRAP v1.0 was discovered to be vulnerable to host header poisoning.	6.1	More Details
CVE-2023-37905	ckeditor-wordcount-plugin is an open source WordCount Plugin for CKEditor. It has been discovered that the `ckeditor-wordcount-plugin` plugin for CKEditor4 is susceptible to cross-site scripting when switching to the source code mode. This issue has been addressed in version 1.17.12 of the `ckeditor-wordcount-plugin` plugin and users are advised to upgrade. There are no known workarounds for this vulnerability.	6.1	More Details
CVE-2023-38496	Apptainer is an open source container platform. Version 1.2.0-rc.2 introduced an ineffective privilege drop when requesting container network setup, therefore subsequent functions are called with root privileges, the attack surface is rather limited for users but an attacker could possibly craft a starter config to delete any directory on the host filesystems. A security fix has been included in Apptainer 1.2.1. There is no known workaround outside of upgrading to Apptainer 1.2.1.	6.1	More Details
CVE-2023-32624	Cross-site scripting vulnerability in TS Webfonts for SAKURA 3.1.0 and earlier allows a remote unauthenticated attacker to inject an arbitrary script.	6.1	More Details
CVE-2023-38617	Office Suite Premium Version v10.9.1.42602 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the filter parameter at /api?path=files.	6.1	More Details
CVE-2023-25841	There is a stored Cross-site Scripting vulnerability in Esri ArcGIS Server versions 10.8.1 – 11.0 on Windows and Linux platforms that may allow a remote, unauthenticated attacker to create crafted content which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. Mitigation: Disable anonymous access to ArcGIS Feature services with edit capabilities.	6.1	More Details
CVE-2021-39425	SeedDMS v6.0.15 was discovered to contain an open redirect vulnerability. An attacker may exploit this vulnerability to redirect users to arbitrary web URLs by tricking the victim users to click on crafted links.	6.1	More Details
CVE-2020-35698	Thinkific Thinkific Online Course Creation Platform 1.0 is affected by: Cross Site Scripting (XSS). The impact is: execute arbitrary code (remote). The component is: Affected Source code of the website CMS which is been used by many to host their online courses using the Thinkific Platform. The attack vector is: To exploit the vulnerability any user has to just visit the link - https://hacktify.thinkific.com/account/billing?success=%E2%80%AA%3Cscript%3Ealert(1)%3C/script%3E. ¶¶ Thinkific is a Website based Learning Platform Product which is used by thousands of users worldwide. There is a Cross Site Scripting (XSS) based vulnerability in the code of the CMS where any attacker can execute a XSS attack. Proof of Concept & Steps to Reproduce: Step1 : Go to Google.com Step 2 : Search for this Dork site:thinkific.com -www Step 3 : You will get a list of websites which are running on the thinkific domains. Step 4 : Create account and signin in any of the website Step 5 : Add this endpoint at the end of the domain and you will see that there is a XSS Alert /account/billing?success=%E2%80%AA<script>alert(1)</script> Step 6 : Choose any domains from google for any website this exploit will work on all the websites as it is a code based flaw in the CMS Step 7 : Thousands of websites are vulnerable due to this vulnerable code in the CMS itself which is giving rise to the XSS attack.	6.1	More Details
CVE-2023-37602	An arbitrary file upload vulnerability in the component /workplace#!explorer of Alkacon OpenCMS v15.0 allows attackers to execute arbitrary code via uploading a crafted PNG file.	6.1	More Details
CVE-2023-3019	A DMA reentrancy issue leading to a use-after-free error was found in the e1000e NIC emulation code in QEMU. This issue could allow a privileged guest user to crash the QEMU process on the host, resulting in a denial of service.	6.0	More Details
CVE-2023-3782	DoS of the OkHttp client when using a BrotliInterceptor and surfing to a malicious web server, or when an attacker can perform MitM to inject a Brotli zip-bomb into an HTTP response	5.9	More Details
CVE-2022-2127	An out-of-bounds read vulnerability was found in Samba due to insufficient length checks in winbindd_pam_auth_crap.c. When performing NTLM authentication, the client replies to cryptographic challenges back to the server. These replies have variable lengths, and Winbind fails to check the lan manager response length. When Winbind is used for NTLM authentication, a maliciously crafted request can trigger an out-of-bounds read in Winbind, possibly resulting in a crash.	5.9	More Details
CVE-2023-34369	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in GrandSlambert Login Configurator plugin <= 2.1 versions.	5.9	More Details
CVE-2023-3323	A vulnerability exists by allowing low-privileged users to read and update the data in various directories used by the Zenon system. An attacker could exploit the vulnerability by using specially crafted programs to exploit the vulnerabilities by allowing them to run on the zenon installed hosts. This issue affects ABB Ability™ zenon: from 11 build through 11 build 106404.	5.9	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-28513	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.3 CD and IBM MQ Appliance 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.2 LTS, under certain configurations, is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 250397.	5.9	More Details
CVE-2021-38933	IBM Sterling Connect:Direct for UNIX 1.5 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 210574.	5.9	More Details
CVE-2023-3347	A vulnerability was found in Samba's SMB2 packet signing mechanism. The SMB2 packet signing is not enforced if an admin configured "server signing = required" or for SMB2 connections to Domain Controllers where SMB2 packet signing is mandatory. This flaw allows an attacker to perform attacks, such as a man-in-the-middle attack, by intercepting the network traffic and modifying the SMB2 messages between client and server, affecting the integrity of the data.	5.9	More Details
CVE-2023-38503	Directus is a real-time API and App dashboard for managing SQL database content. Starting in version 10.3.0 and prior to version 10.5.0, the permission filters (i.e. `user_created IS $CURRENT_USER`) are not properly checked when using GraphQL subscription resulting in unauthorized users getting event on their subscription which they should not be receiving according to the permissions. This can be any collection but out-of-the box the `directus_users` collection is configured with such a permissions filter allowing you to get updates for other users when changes happen. Version 10.5.0 contains a patch. As a workaround, disable GraphQL subscriptions.	5.7	More Details
CVE-2023-3793	A vulnerability was found in Weaver e-cology. It has been rated as critical. This issue affects some unknown processing of the file filelFileDownloadForOutDoc.class of the component HTTP POST Request Handler. The manipulation of the argument fileid with the input 1+WAITFOR+DELAY leads to sql injection. Upgrading to version 10.58.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-235061 was assigned to this vulnerability.	5.5	More Details
CVE-2023-39129	GNU gdb (GDB) 13.0.50.20220805-git was discovered to contain a heap use after free via the function add_pe_exported_sym() at /gdb/coff-pe-read.c.	5.5	More Details
CVE-2023-3745	A heap-based buffer overflow issue was found in ImageMagick's PushCharPixel() function in quantum-private.h. This issue may allow a local attacker to trick the user into opening a specially crafted file, triggering an out-of-bounds read error and allowing an application to crash, resulting in a denial of service.	5.5	More Details
CVE-2023-3804	A vulnerability classified as problematic was found in Chengdu Flash Flood Disaster Monitoring and Warning System 2.0. This vulnerability affects unknown code of the file /Service/FileHandler.ashx. The manipulation of the argument userFile leads to unrestricted upload. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-235072. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-32446	Dell Wyse ThinOS versions prior to 2303 (9.4.1141) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files.	5.5	More Details
CVE-2023-32447	Dell Wyse ThinOS versions prior to 2306 (9.4.2103) contain a sensitive information disclosure vulnerability. A malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files.	5.5	More Details
CVE-2023-32455	Dell Wyse ThinOS versions prior to 2208 (9.3.2102) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files.	5.5	More Details
CVE-2023-38633	A directory traversal problem in the URL decoder of librsvg before 2.56.3 could be used by local or remote attackers to disclose files (on the local filesystem outside of the expected area), as demonstrated by href=".?../../../../../../../../../../etc/passwd" in an xi:include element.	5.5	More Details
CVE-2023-3802	A vulnerability was found in Chengdu Flash Flood Disaster Monitoring and Warning System 2.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /Controller/Ajaxfileupload.ashx. The manipulation of the argument file leads to unrestricted upload. The exploit has been disclosed to the public and may be used. VDB-235070 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-3772	A flaw was found in the Linux kernel's IP framework for transforming packets (XFRM subsystem). This issue may allow a malicious user with CAP_NET_ADMIN privileges to directly dereference a NULL pointer in xfrm_update_ae_params(), leading to a possible kernel crash and denial of service.	5.5	More Details
CVE-2023-3773	A flaw was found in the Linux kernel's IP framework for transforming packets (XFRM subsystem). This issue may allow a malicious user with CAP_NET_ADMIN privileges to cause a 4 byte out-of-bounds read of XFRMA_MTIMER_THRESH when parsing netlink attributes, leading to potential leakage of sensitive heap data to userspace.	5.5	More Details
CVE-2023-37748	ngiflib commit 5e7292 was discovered to contain an infinite loop via the function DecodeGifImg at ngiflib.c.	5.5	More Details
CVE-2022-40896	A ReDoS issue was discovered in pygments/lexers/smithy.py in pygments through 2.15.0 via SmithyLexer.	5.5	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-3798	A vulnerability has been found in Chengdu Flash Flood Disaster Monitoring and Warning System 2.0 and classified as critical. This vulnerability affects unknown code of the file /App_Resource/UEditor/server/upload.aspx. The manipulation of the argument file leads to unrestricted upload. The exploit has been disclosed to the public and may be used. VDB-235066 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-39128	GNU gdb (GDB) 13.0.50.20220805-git was discovered to contain a stack overflow via the function ada_decode at /gdb/ada-lang.c.	5.5	More Details
CVE-2023-3801	A vulnerability was found in IBOS OA 4.5.5. It has been declared as critical. Affected by this vulnerability is the function actionEdit of the file ?r=officialdoc/officialdoc/edit of the component Mobile Notification Handler. The manipulation leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-235069 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-39130	GNU gdb (GDB) 13.0.50.20220805-git was discovered to contain a heap buffer overflow via the function pe_as16() at /gdb/coff-pe-read.c.	5.5	More Details
CVE-2023-32635	XBRL data create application version 7.0 and earlier improperly restricts XML external entity references (XXE). By processing a specially crafted XBRL file, arbitrary files on the system may be read by an attacker.	5.5	More Details
CVE-2023-3797	A vulnerability, which was classified as critical, was found in Gen Technology Four Mountain Torrent Disaster Prevention and Control of Monitoring and Early Warning System up to 20230712. This affects an unknown part of the file /Duty/AjaxHandle/UploadFloodPlanFileUpdate.ashx. The manipulation of the argument Filedata leads to unrestricted upload. The exploit has been disclosed to the public and may be used. The identifier VDB-235065 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-3795	A vulnerability classified as critical was found in Bug Finder ChainCity Real Estate Investment Platform 1.0. Affected by this vulnerability is an unknown functionality of the file /property of the component GET Parameter Handler. The manipulation of the argument name leads to sql injection. The associated identifier of this vulnerability is VDB-235063. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-32639	Applicant Programme Ver.7.06 and earlier improperly restricts XML external entity references (XXE). By processing a specially crafted XML file, arbitrary files on the system may be read by an attacker.	5.5	More Details
CVE-2023-20593	An issue in “Zen 2” CPUs, under specific microarchitectural circumstances, may allow an attacker to potentially access sensitive information.	5.5	More Details
CVE-2023-2430	A vulnerability was found due to missing lock for IOPOLL flaw in io_cqring_event_overflow() in io_uring.c in Linux Kernel. This flaw allows a local attacker with user privilege to trigger a Denial of Service threat.	5.5	More Details
CVE-2023-35929	Tuleap is a free and open source suite to improve management of software development and collaboration. Prior to version 14.10.99.4 of Tuleap Community Edition and prior to versions 14.10-2 and 14.9-5 of Tuleap Enterprise Edition, content displayed in the "card fields" (visible in the kanban and PV2 apps) is not properly escaped. A malicious user with the capability to create an artifact or to edit a field used as a card field could force victim to execute uncontrolled code. Tuleap Community Edition 14.10.99.4, Tuleap Enterprise Edition 14.10-2, and Tuleap Enterprise Edition 14.9-5 contain a fix.	5.4	More Details
CVE-2023-25836	There is a Cross-site Scripting vulnerability in Esri Portal Sites in versions 10.8.1 – 10.9 that may allow a remote, authenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victims browser. The privileges required to execute this attack are low.	5.4	More Details
CVE-2023-3384	A flaw was found in the Quay registry. While the image labels created through Quay undergo validation both in the UI and backend by applying a regex (validation.py), the same validation is not performed when the label comes from an image. This flaw allows an attacker to publish a malicious image to a public registry containing a script that can be executed via Cross-site scripting (XSS).	5.4	More Details
CVE-2023-3821	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.6.4.	5.4	More Details
CVE-2022-28867	An issue was discovered in Nokia NetAct 22 through the Administration of Measurements website section. A malicious user can edit or add the templateName parameter in order to include JavaScript code, which is then stored and executed by a victim's web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or e-mailed directly to victims. Here, the /aom/html/EditTemplate.jsf and /aom/html/ViewAllTemplatesPage.jsf templateName parameter is used.	5.4	More Details
CVE-2022-28865	An issue was discovered in Nokia NetAct 22 through the Site Configuration Tool website section. A malicious user can change a filename of an uploaded file to include JavaScript code, which is then stored and executed by a victim's web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or e-mailed directly to victims. Here, the /netact/sct filename parameter is used.	5.4	More Details
CVE-2023-39173	In JetBrains TeamCity before 2023.05.2 a token with limited permissions could be used to gain full account access	5.4	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-37901	Indico is an open source a general-purpose, web based event management tool. There is a Cross-Site-Scripting vulnerability in confirmation prompts commonly used when deleting content from Indico. Exploitation requires someone with at least submission privileges (such as a speaker) and then someone else to attempt to delete this content. Considering that event organizers may want to delete suspicious-looking content when spotting it, there is a non-negligible risk of such an attack to succeed. The risk of this could be further increased when combined with some some social engineering pointing the victim towards this content. Users need to update to Indico 3.2.6 as soon as possible. See the docs for instructions on how to update. Users who cannot upgrade should only let trustworthy users manage categories, create events or upload materials ("submission" privileges on a contribution/event). This should already be the case in a properly-configured setup when it comes to category/event management. Note that a conference doing a Call for Abstracts actively invites external speakers (who the organizers may not know and thus cannot fully trust) to submit content, hence the need to update to a a fixed version ASAP in particular when using such workflows.	5.4	More Details
CVE-2021-45094	Imprivata Privileged Access Management (formally Xton Privileged Access Management) 2.3.202112051108 allows XSS.	5.4	More Details
CVE-2023-37257	DataEase is an open source data visualization analysis tool. Prior to version 1.18.9, the DataEase panel and dataset have a stored cross-site scripting vulnerability. The vulnerability has been fixed in v1.18.9. There are no known workarounds.	5.4	More Details
CVE-2023-28530	IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials. IBM X-Force ID: 251214.	5.4	More Details
CVE-2023-37645	eyoucms v1.6.3 was discovered to contain an information disclosure vulnerability via the component /custom_model_path/recruit.filelist.txt.	5.3	More Details
CVE-2023-34968	A path disclosure vulnerability was found in Samba. As part of the Spotlight protocol, Samba discloses the server-side absolute path of shares, files, and directories in the results for search queries. This flaw allows a malicious client or an attacker with a targeted RPC request to view the information that is part of the disclosed path.	5.3	More Details
CVE-2023-34967	A Type Confusion vulnerability was found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets, one encoded data structure is a key-value style dictionary where the keys are character strings, and the values can be any of the supported types in the mdssvc protocol. Due to a lack of type checking in callers of the dalloc_value_for_key() function, which returns the object associated with a key, a caller may trigger a crash in talloc_get_size() when talloc detects that the passed-in pointer is not a valid talloc pointer. With an RPC worker process shared among multiple client connections, a malicious client or attacker can trigger a process crash in a shared RPC mdssvc worker process, affecting all other clients this worker serves.	5.3	More Details
CVE-2023-38335	Omnis Studio 10.22.00 has incorrect access control. It advertises a feature for making Omnis libraries "always private" - this is supposed to be an irreversible operation. However, due to implementation issues, "always private" Omnis libraries can be opened by the Omnis Studio browser by bypassing specific checks. This violates the expected behavior of an "irreversible operation".	5.3	More Details
CVE-2023-3102	A sensitive information leak issue has been discovered in GitLab EE affecting all versions starting from 16.0 before 16.0.6, all versions starting from 16.1 before 16.1.1, which allows access to titles of private issue and MR.	5.3	More Details
CVE-2023-33777	An issue in /functions/fbaorder.php of Prestashop amazon before v5.2.24 allows attackers to execute a directory traversal attack.	5.3	More Details
CVE-2023-38523	The web interface on multiple Samsung Harman AMX N-Series devices allows directory listing for the /tmp/ directory, without authentication, exposing sensitive information such as the command history and screenshot of the file being processed. This affects N-Series N1115 Wallplate Video Encoder before 1.15.61, N-Series N1x22A Video Encoder/Decoder before 1.15.61, N-Series N1x33A Video Encoder/Decoder before 1.15.61, N-Series N1x33 Video Encoder/Decoder before 1.15.61, N-Series N2x35 Video Encoder/Decoder before 1.15.61, N-Series N2x35A Video Encoder/Decoder before 1.15.61, N-Series N2xx2 Video Encoder/Decoder before 1.15.61, N-Series N2xx2A Video Encoder/Decoder before 1.15.61, N-Series N3000 Video Encoder/Decoder before 2.12.105, and N-Series N4321 Audio Transceiver before 1.00.06.	5.3	More Details
CVE-2023-3300	HashiCorp Nomad and Nomad Enterprise 0.11.0 up to 1.5.6 and 1.4.1 HTTP search API can reveal names of available CSI plugins to unauthenticated users or users without the plugin:read policy. Fixed in 1.6.0, 1.5.7, and 1.4.1.	5.3	More Details
CVE-2023-26026	Planning Analytics Cartridge for Cloud Pak for Data 4.0 exposes sensitive information in logs which could lead an attacker to exploit this vulnerability to conduct further attacks. IBM X-Force ID: 247896.	5.3	More Details
CVE-2023-27877	IBM Planning Analytics Cartridge for Cloud Pak for Data 4.0 connects to a CouchDB server. An attacker can exploit an insecure password policy to the CouchDB server and collect sensitive information from the database. IBM X-Force ID: 247905.	5.3	More Details
CVE-2023-37902	Vyper is a Pythonic programming language that targets the Ethereum Virtual Machine (EVM). Prior to version 0.3.10, the ecrecover precompile does not fill the output buffer if the signature does not verify. However, the ecrecover builtin will still return whatever is at memory location 0. This means that the if the compiler has been convinced to write to the 0 memory location with specially crafted data (generally, this can happen with a hashmap access or immutable read) just before the ecrecover, a signature check might pass on an invalid signature. Version 0.3.10 contains a patch for this issue.	5.3	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-3779	The Essential Addons For Elementor plugin for WordPress is vulnerable to unauthenticated API key disclosure in versions up to, and including, 5.8.1 due to the plugin adding the API key to the source code of any page running the MailChimp block. This makes it possible for unauthenticated attackers to obtain a site's MailChimp API key. We recommend resetting any MailChimp API keys if running a vulnerable version of this plugin with the MailChimp block enabled as the API key may have been compromised. This only affects sites running the premium version of the plugin and that have the Mailchimp block enabled on a page.	5.3	More Details
CVE-2023-3446	Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulernable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.	5.3	More Details
CVE-2023-32657	Weintek Weincloud v0.13.6 could allow an attacker to efficiently develop a brute force attack on credentials with authentication hints from error message responses.	5.3	More Details
CVE-2023-37276	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. aiohttp v3.8.4 and earlier are bundled with llhttp v6.0.6. Vulnerable code is used by aiohttp for its HTTP request parser when available which is the default case when installing from a wheel. This vulnerability only affects users of aiohttp as an HTTP server (ie `aiohttp.Application`), you are not affected by this vulnerability if you are using aiohttp as an HTTP client library (ie `aiohttp.ClientSession`). Sending a crafted HTTP request will cause the server to misinterpret one of the HTTP header values leading to HTTP request smuggling. This issue has been addressed in version 3.8.5. Users are advised to upgrade. Users unable to upgrade can reinstall aiohttp using `AIOHTTP_NO_EXTENSIONS=1` as an environment variable to disable the llhttp HTTP request parser implementation. The pure Python implementation isn't vulnerable.	5.3	More Details
CVE-2023-32481	Wyse Management Suite versions prior to 4.0 contain a denial-of-service vulnerability. An authenticated malicious user can flood the configured SMTP server with numerous requests in order to deny access to the system.	4.9	More Details
CVE-2023-32482	Wyse Management Suite versions prior to 4.0 contain an improper authorization vulnerability. An authenticated malicious user with privileged access can push policies to unauthorized tenant group.	4.9	More Details
CVE-2023-38195	Datalust Seq before 2023.2.9489 allows insertion of sensitive information into an externally accessible file or directory. This is exploitable only when external (SQL Server or PostgreSQL) metadata storage is used. Exploitation can only occur from a high-privileged user account.	4.9	More Details
CVE-2023-3344	The Auto Location for WP Job Manager via Google WordPress plugin before 1.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-3248	The All-in-one Floating Contact Form WordPress plugin before 2.1.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-3897	Username enumeration is possible through Bypassing CAPTCHA in On-premise SureMDM Solution on Windows deployment allows attacker to enumerate local user information via error message. This issue affects SureMDM On-premise: 6.31 and below version	4.8	More Details
CVE-2023-34093	Strapi is an open-source headless content management system. Prior to version 4.10.8, anyone (Strapi developers, users, plugins) can make every attribute of a Content-Type public without knowing it. The vulnerability only affects the handling of content types by Strapi, not the actual content types themselves. Users can use plugins or modify their own content types without realizing that the `privateAttributes` getter is being removed, which can result in any attribute becoming public. This can lead to sensitive information being exposed or the entire system being taken control of by an attacker(having access to password hashes). Anyone can be impacted, depending on how people are using/extending content-types. If the users are mutating the content-type, they will not be affected. Version 4.10.8 contains a patch for this issue.	4.8	More Details
CVE-2023-38500	TYPO3 HTML Sanitizer is an HTML sanitizer, written in PHP, aiming to provide cross-site-scripting-safe markup based on explicitly allowed tags, attributes and values. Starting in version 1.0.0 and prior to versions 1.5.1 and 2.1.2, due to an encoding issue in the serialization layer, malicious markup nested in a `noscript` element was not encoded correctly. `noscript` is disabled in the default configuration, but might have been enabled in custom scenarios. This allows bypassing the cross-site scripting mechanism of TYPO3 HTML Sanitizer. Versions 1.5.1 and 2.1.2 fix the problem.	4.7	More Details
CVE-2023-2850	NodeBB is affected by a Cross-Site WebSocket Hijacking vulnerability due to missing validation of the request origin. Exploitation of this vulnerability allows certain user information to be extracted by attacker.	4.7	More Details
CVE-2023-3852	A vulnerability was found in OpenRapid RapidCMS up to 1.3.1. It has been declared as critical. This vulnerability affects unknown code of the file /admin/upload.php. The manipulation of the argument file leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 4dff387283060961c362d50105ff8da8ea40bcbe. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-235204.	4.7	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-35392	Microsoft Edge (Chromium-based) Spoofing Vulnerability	4.7	More Details
CVE-2023-25929	IBM Cognos Analytics 11.1 and 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247861.	4.6	More Details
CVE-2023-39175	In JetBrains TeamCity before 2023.05.2 reflected XSS via GitHub integration was possible	4.6	More Details
CVE-2023-2860	An out-of-bounds read vulnerability was found in the SR-IPv6 implementation in the Linux kernel. The flaw exists within the processing of seg6 attributes. The issue results from the improper validation of user-supplied data, which can result in a read past the end of an allocated buffer. This flaw allows a privileged local user to disclose sensitive information on affected installations of the Linux kernel.	4.4	More Details
CVE-2023-32483	Wyse Management Suite versions prior to 4.0 contain a sensitive information disclosure vulnerability. An authenticated malicious user having local access to the system running the application could exploit this vulnerability to read sensitive information written to log files.	4.4	More Details
CVE-2023-39174	In JetBrains TeamCity before 2023.05.2 a ReDoS attack was possible via integration with issue trackers	4.3	More Details
CVE-2023-35898	IBM InfoSphere Information Server 11.7 could allow an authenticated user to obtain sensitive information due to an insecure security configuration in InfoSphere Data Flow Designer. IBM X-Force ID: 259352.	4.3	More Details
CVE-2023-35900	IBM Robotic Process Automation for Cloud Pak 21.0.0 through 21.0.7.4 and 23.0.0 through 23.0.5 is vulnerable to disclosing server version information which may be used to determine software vulnerabilities at the operating system level. IBM X-Force ID: 259368.	4.3	More Details
CVE-2022-43908	IBM Security Guardium 11.3 could allow an authenticated user to cause a denial of service due to improper input validation. IBM X-Force ID: 240903.	4.3	More Details
CVE-2023-3760	A vulnerability has been found in Intergard SGS 8.7.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Change Password Handler. The manipulation leads to denial of service. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-234445 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-3762	A vulnerability was found in Intergard SGS 8.7.0. It has been classified as problematic. This affects an unknown part. The manipulation leads to cleartext storage of sensitive information in memory. 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-234447. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-3792	A vulnerability was found in Beijing Netcon NS-ASG 6.3. It has been classified as problematic. This affects an unknown part of the file /admin/test_status.php. The manipulation leads to direct request. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235059. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-3786	A vulnerability classified as problematic has been found in Aures Komet up to 20230509. This affects an unknown part of the component Kiosk Mode. The manipulation leads to improper access controls. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. The identifier VDB-235053 was assigned to this vulnerability.	4.3	More Details
CVE-2023-32262	A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability allows attackers with Item/Configure permission to access and capture credentials they are not entitled to. See the following Jenkins security advisory for details: * https://www.jenkins.io/security/advisory/2023-06-14/ https://www.jenkins.io/security/advisory/2023-06-14/	4.3	More Details
CVE-2023-3637	An uncontrolled resource consumption flaw was found in openstack-neutron. This flaw allows a remote authenticated user to query a list of security groups for an invalid project. This issue creates resources that are unconstrained by the user's quota. If a malicious user were to submit a significant number of requests, this could lead to a denial of service.	4.3	More Details
CVE-2023-3841	A vulnerability has been found in NxFilter 4.3.2.5 and classified as problematic. This vulnerability affects unknown code of the file user.jsp. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The identifier of this vulnerability is VDB-235192. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-23568	Improper privilege validation in Command Centre Server allows authenticated unprivileged operators to modify and view Personal Data Fields. This issue affects Command Centre: vEL 8.90 prior to vEL8.90.1318 (MR1), vEL8.80 prior to vEL8.80.1192 (MR2), vEL8.70 prior to vEL8.70.2185 (MR4), vEL8.60 prior to vEL8.60.2347 (MR6), vEL8.50 prior to vEL8.50.2831 (MR8), all versions vEL8.40 and prior	4.3	More Details
CVE-2023-3796	A vulnerability, which was classified as problematic, has been found in Bug Finder Foody Friend 1.0. Affected by this issue is some unknown functionality of the file /user/profile of the component Profile Picture Handler. The manipulation of the argument profile_picture leads to unrestricted upload. The attack may be launched remotely. The identifier of this vulnerability is VDB-235064. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-32625	Cross-site request forgery (CSRF) vulnerability in TS Webfonts for SAKURA 3.1.2 and earlier allows a remote unauthenticated attacker to hijack the authentication of a user and to change settings by having a user view a malicious page.	4.3	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-38173	Microsoft Edge for Android Spoofing Vulnerability	4.3	More Details
CVE-2023-32261	A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. See the following Jenkins security advisory for details: * https://www.jenkins.io/security/advisory/2023-06-14/ https://www.jenkins.io/security/advisory/2023-06-14/	4.2	More Details
CVE-2023-3839	A vulnerability, which was classified as problematic, has been found in DedeBIZ 6.2.10. Affected by this issue is some unknown functionality of the file /admin/sys_sql_query.php. The manipulation of the argument sqlquery leads to sql injection. The attack may 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. VDB-235190 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.1	More Details
CVE-2023-38057	An improper input validation vulnerability in OTRS Survey modules allows any attacker with a link to a valid and unanswered survey request to inject javascript code in free text answers. This allows a cross site scripting attack while reading the replies as authenticated agent. This issue affects OTRS Survey module from 7.0.X before 7.0.32, from 8.0.X before 8.0.13 and ((OTRS)) Community Edition Survey module from 6.0.X through 6.0.22.	4.1	More Details
CVE-2023-3072	HashiCorp Nomad and Nomad Enterprise 0.7.0 up to 1.5.6 and 1.4.10 ACL policies using a block without a label generates unexpected results. Fixed in 1.6.0, 1.5.7, and 1.4.11.	4.1	More Details
CVE-2023-38058	An improper privilege check in the OTRS ticket move action in the agent interface allows any as agent authenticated attacker to to perform a move of an ticket without the needed permission. This issue affects OTRS: from 8.0.X before 8.0.35.	4.1	More Details
CVE-2023-3800	A vulnerability was found in EasyAdmin8 2.0.2.2. It has been classified as problematic. Affected is an unknown function of the file /admin/index/index.html#/admin/mall.goods/index.html of the component File Upload Module. The manipulation leads to unrestricted upload. 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 used. The identifier of this vulnerability is VDB-235068. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.9	More Details
CVE-2023-3763	A vulnerability was found in Intergard SGS 8.7.0. It has been declared as problematic. This vulnerability affects unknown code of the component SQL Query Handler. The manipulation leads to cleartext transmission of sensitive information. The attack can be 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 identifier of this vulnerability is VDB-234448. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2023-38499	TYPO3 is an open source PHP based web content management system. Starting in version 9.4.0 and prior to versions 9.5.42 ELTS, 10.4.39 ELTS, 11.5.30, and 12.4.4, in multi-site scenarios, enumerating the HTTP query parameters `id` and `L` allowed out-of-scope access to rendered content in the website frontend. For instance, this allowed visitors to access content of an internal site by adding handcrafted query parameters to the URL of a site that was publicly available. TYPO3 versions 9.5.42 ELTS, 10.4.39 ELTS, 11.5.30, 12.4.4 fix the problem.	3.7	More Details
CVE-2023-3761	A vulnerability was found in Intergard SGS 8.7.0 and classified as problematic. Affected by this issue is some unknown functionality of the component Password Change Handler. The manipulation leads to cleartext transmission of sensitive information. The attack may 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. VDB-234446 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2023-29259	IBM Sterling Connect:Express for UNIX 1.5 browser UI is vulnerable to attacks that rely on the use of cookies without the SameSite attribute. IBM X-Force ID: 252055.	3.7	More Details
CVE-2023-3856	A vulnerability, which was classified as problematic, has been found in phpscriptpoint Ecommerce 1.15. Affected by this issue is some unknown functionality of the file /blog-single.php. The manipulation of the argument slug leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-235208. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3855	A vulnerability classified as problematic was found in phpscriptpoint JobSeeker 1.5. Affected by this vulnerability is an unknown functionality of the file /search-result.php. The manipulation of the argument kw/lc/ct/cp/p leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-235207. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3835	A vulnerability classified as problematic has been found in Bug Finder MineStack 1.0. This affects an unknown part of the file /user/ticket/create of the component Ticket Handler. The manipulation of the argument message leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-235161 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3857	A vulnerability, which was classified as problematic, was found in phpscriptpoint Ecommerce 1.15. This affects an unknown part of the file /product.php. The manipulation of the argument id leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-235209 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3853	A vulnerability was found in phpscriptpoint BloodBank 1.1. It has been rated as problematic. This issue affects some unknown processing of the file page.php. The manipulation leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-235205 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-3860	A vulnerability was found in phpscriptpoint Insurance 1.2. It has been classified as problematic. Affected is an unknown function of the file /page.php. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-235212. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3861	A vulnerability was found in phpscriptpoint Insurance 1.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /search.php. The manipulation leads to cross site scripting. The attack can be launched remotely. The identifier VDB-235213 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3858	A vulnerability has been found in phpscriptpoint Car Listing 1.6 and classified as problematic. This vulnerability affects unknown code of the file /search.php. The manipulation of the argument country/state/city leads to cross site scripting. The attack can be initiated remotely. VDB-235210 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3755	A vulnerability has been found in Creativeitem Atlas Business Directory Listing 2.13 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /home/filter_listings. The manipulation of the argument price-range leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-234427. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3757	A vulnerability classified as problematic has been found in GZ Scripts Car Rental Script 1.8. Affected is an unknown function of the file /EventBookingCalendar/load.php?controller=GzFront/action=checkout/cid=1/layout=calendar/show_header=T/local=3. The manipulation of the argument first_name/second_name/phone/address_1/country leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-234432. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3756	A vulnerability was found in Creativeitem Atlas Business Directory Listing 2.13 and classified as problematic. Affected by this issue is some unknown functionality of the file /home/search. The manipulation of the argument search_string leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-234428. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3840	A vulnerability, which was classified as problematic, was found in NxFilter 4.3.2.5. This affects an unknown part of the file /report,daily.jsp?stime=2023%2F07%2F12&timeOption=yesterday&. The manipulation of the argument user leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-235191. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3754	A vulnerability, which was classified as problematic, was found in Creativeitem Ekushey Project Manager CRM 5.0. Affected is an unknown function of the file /index.php/client/message/message_read/xxxxxxxx[random-msg-hash]. The manipulation of the argument message leads to cross site scripting. It is possible to launch the attack remotely. VDB-234426 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3944	A vulnerability was found in phpscriptpoint Lawyer 1.6 and classified as problematic. Affected by this issue is some unknown functionality of the file page.php. The manipulation leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-235400. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3849	A vulnerability, which was classified as problematic, was found in mooSocial mooDating 1.2. Affected is an unknown function of the file /find-a-match of the component URL Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-235200. NOTE: We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	3.5	More Details
CVE-2023-3753	A vulnerability classified as problematic has been found in Creativeitem Mastery LMS 1.2. This affects an unknown part of the file /browse. The manipulation of the argument search/featured/recommended/skill leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-234423. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3752	A vulnerability was found in Creativeitem Academy LMS 5.15. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /home/courses. The manipulation of the argument sort_by leads to cross site scripting. The attack may be launched remotely. VDB-234422 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3848	A vulnerability, which was classified as problematic, has been found in mooSocial mooDating 1.2. This issue affects some unknown processing of the file /users/view of the component URL Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-235199. NOTE: We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	3.5	More Details
CVE-2023-3847	A vulnerability classified as problematic was found in mooSocial mooDating 1.2. This vulnerability affects unknown code of the file /users of the component URL Handler. The manipulation leads to cross site scripting. The attack can be initiated remotely. VDB-235198 is the identifier assigned to this vulnerability. NOTE: We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	3.5	More Details
CVE-2023-3846	A vulnerability classified as problematic has been found in mooSocial mooDating 1.2. This affects an unknown part of the file /pages of the component URL Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-235197 was assigned to this vulnerability. NOTE: We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	3.5	More Details
CVE-2023-3845	A vulnerability was found in mooSocial mooDating 1.2. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /friends/ajax_invite of the component URL Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-235196. NOTE: We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	3.5	More Details
CVE-2023-3844	A vulnerability was found in mooSocial mooDating 1.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /friends of the component URL Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-235195. NOTE: We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	3.5	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-3843	A vulnerability was found in mooSocial mooDating 1.2. It has been classified as problematic. Affected is an unknown function of the file /matchmakings/question of the component URL Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. VDB-235194 is the identifier assigned to this vulnerability. NOTE: We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	3.5	More Details
CVE-2023-3945	A vulnerability was found in phpscriptpoint Lawyer 1.6. It has been classified as problematic. This affects an unknown part of the file search.php. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-235401 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3834	A vulnerability was found in Bug Finder EX-RATE 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /user/ticket/create of the component Ticket Handler. The manipulation of the argument message leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-235160. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3833	A vulnerability was found in Bug Finder Montage 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /user/ticket/create of the component Ticket Handler. The manipulation of the argument message leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-235159. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3832	A vulnerability was found in Bug Finder Wedding Wonders 1.0. It has been classified as problematic. Affected is an unknown function of the file /user/ticket/create of the component Ticket Handler. The manipulation of the argument message leads to cross site scripting. It is possible to launch the attack remotely. VDB-235158 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3815	A vulnerability, which was classified as problematic, has been found in y_project RuoYi up to 4.7.7. Affected by this issue is the function uploadFilesPath of the component File Upload. The manipulation of the argument originalFilenames leads to cross site scripting. The attack may be launched remotely. VDB-235118 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-3794	A vulnerability classified as problematic has been found in Bug Finder ChainCity Real Estate Investment Platform 1.0. Affected is an unknown function of the file /chaincity/user/ticket/create of the component New Ticket Handler. The manipulation of the argument subject leads to cross site scripting. It is possible to launch the attack remotely. VDB-235062 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3790	A vulnerability has been found in Boom CMS 8.0.7 and classified as problematic. Affected by this vulnerability is the function add of the component assets-manager. The manipulation of the argument title/description leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-235057 was assigned to this vulnerability.	3.5	More Details
CVE-2023-3789	A vulnerability, which was classified as problematic, was found in PaulPrinting CMS 2018. Affected is an unknown function of the file /account/delivery of the component Search. The manipulation of the argument s leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-235056.	3.5	More Details
CVE-2023-3788	A vulnerability, which was classified as problematic, has been found in ActiveITzone Active Super Shop CMS 2.5. This issue affects some unknown processing of the component Manage Details Page. The manipulation of the argument name/phone/address leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235055.	3.5	More Details
CVE-2023-3787	A vulnerability classified as problematic was found in Codecanyon Tiva Events Calender 1.4. This vulnerability affects unknown code. The manipulation of the argument name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-235054 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-3883	A vulnerability, which was classified as problematic, was found in Campcodes Beauty Salon Management System 1.0. This affects an unknown part of the file /admin/add-category.php. The manipulation of the argument name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-235245 was assigned to this vulnerability.	3.5	More Details
CVE-2023-3884	A vulnerability has been found in Campcodes Beauty Salon Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/edit_product.php. The manipulation of the argument id leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-235246 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-3885	A vulnerability was found in Campcodes Beauty Salon Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /admin/edit_category.php. The manipulation of the argument id leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235247.	3.5	More Details
CVE-2023-3886	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file /admin/invoice.php. The manipulation of the argument inv_id leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-235248.	3.5	More Details
CVE-2023-3887	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/search-appointment.php. The manipulation of the argument searchdata leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-235249 was assigned to this vulnerability.	3.5	More Details
CVE-2023-3888	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/admin-profile.php. The manipulation of the argument adminname leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-235250 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-3890	A vulnerability classified as problematic has been found in Campcodes Beauty Salon Management System 1.0. This affects an unknown part of the file /admin/edit-accepted-appointment.php. The manipulation of the argument id leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235251.	3.5	More Details
CVE-2023-3831	A vulnerability was found in Bug Finder Finounce 1.0 and classified as problematic. This issue affects some unknown processing of the file /user/ticket/create of the component Ticket Handler. The manipulation of the argument message leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-235157 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3748	A flaw was found in FRRouting when parsing certain babeld unicast hello messages that are intended to be ignored. This issue may allow an attacker to send specially crafted hello messages with the unicast flag set, the interval field set to 0, or any TLV that contains a sub-TLV with the Mandatory flag set to enter an infinite loop and cause a denial of service.	3.5	More Details
CVE-2023-3828	A vulnerability was found in Bug Finder Listplace Directory Listing Platform 3.0. It has been classified as problematic. This affects an unknown part of the file /listplace/user/coverPhotoUpdate of the component Photo Handler. The manipulation of the argument user_cover_photo leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-235149 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3830	A vulnerability was found in Bug Finder SASS BILLER 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /company/store. The manipulation of the argument name leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-235151. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3785	A vulnerability was found in PaulPrinting CMS 2018. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument firstname/lastname/address/city/state leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-235052.	3.5	More Details
CVE-2023-3827	A vulnerability was found in Bug Finder Listplace Directory Listing Platform 3.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /listplace/user/ticket/create of the component HTTP POST Request Handler. The manipulation of the argument message leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-235148. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3784	A vulnerability was found in Dooblou WiFi File Explorer 1.13.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument search/order/download/mode leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235051.	3.5	More Details
CVE-2023-3783	A vulnerability was found in Webile 1.0.1. It has been classified as problematic. Affected is an unknown function of the component HTTP POST Request Handler. The manipulation of the argument new_file_name/c leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-235050 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-3829	A vulnerability was found in Bug Finder ICOGenie 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /user/ticket/create of the component Support Ticket Handler. The manipulation of the argument message leads to cross site scripting. The attack can be initiated remotely. VDB-235150 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-25840	There is a Cross-site Scripting vulnerability in ArcGIS Server in versions 10.8.1 – 11.1 that may allow a remote, authenticated attacker to create a crafted link which onmouseover wont execute but could potentially render an image in the victims browser. The privileges required to execute this attack are high.	3.4	More Details
CVE-2023-3299	HashiCorp Nomad Enterprise 1.2.11 up to 1.5.6, and 1.4.10 ACL policies using a block without a label generates unexpected results. Fixed in 1.6.0, 1.5.7, and 1.4.11.	3.4	More Details
CVE-2023-1386	A flaw was found in the 9p passthrough filesystem (9pfs) implementation in QEMU. When a local user in the guest writes an executable file with SUID or SGID, none of these privileged bits are correctly dropped. As a result, in rare circumstances, this flaw could be used by malicious users in the guest to elevate their privileges within the guest and help a host local user to elevate privileges on the host.	3.3	More Details
CVE-2023-3603	A missing allocation check in sftp server processing read requests may cause a NULL dereference on low-memory conditions. The malicious client can request up to 4GB SFTP reads, causing allocation of up to 4GB buffers, which was not being checked for failure. This will likely crash the authenticated user's sftp server connection (if implemented as forking as recommended). For thread-based servers, this might also cause DoS for legitimate users. Given this code is not in any released versions, no security releases have been issued.	3.1	More Details
CVE-2023-3862	A vulnerability was found in Travelmate Travelable Trek Management Solution 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Comment Box Handler. The manipulation of the argument comment leads to cross site scripting. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. VDB-235214 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2023-37361	REDCap 12.0.26 LTS and 12.3.2 Standard allows SQL Injection via scheduling, repeatforms, purpose, app_title, or randomization.	2.7	More Details
CVE-2023-3803	A vulnerability classified as problematic has been found in Chengdu Flash Flood Disaster Monitoring and Warning System 2.0. This affects an unknown part of the file /Service/ImageStationDataService.asmx of the component File Name Handler. The manipulation leads to insufficiently random values. 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 used. The associated identifier of this vulnerability is VDB-235071. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.6	More Details

CVE Number	Description	Base Score	Refere
CVE-2023-32263	A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability could be exploited to retrieve a login certificate if an authenticated user is duped into using an attacker-controlled Dimensions CM server. This vulnerability only applies when the Jenkins plugin is configured to use login certificate credentials. https://www.jenkins.io/security/advisory/2023-06-14/	2.6	More Details
CVE-2023-3247	In PHP versions 8.0.* before 8.0.29, 8.1.* before 8.1.20, 8.2.* before 8.2.7 when using SOAP HTTP Digest Authentication, random value generator was not checked for failure, and was using narrower range of values than it should have. In case of random generator failure, it could lead to a disclosure of 31 bits of uninitialized memory from the client to the server, and it also made easier to a malicious server to guess the client's nonce.	2.6	More Details
CVE-2023-3837	A vulnerability classified as problematic has been found in DedeBIZ 6.2.10. Affected is an unknown function of the file /admin/sys_sql_query.php. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-235188. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2023-3838	A vulnerability classified as problematic was found in DedeBIZ 6.2.10. Affected by this vulnerability is an unknown functionality of the file /admin/vote_edit.php. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-235189 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2023-3674	A flaw was found in the keylime attestation verifier, which fails to flag a device's submitted TPM quote as faulty when the quote's signature does not validate for some reason. Instead, it will only emit an error in the log without flagging the device as untrusted.	2.3	More Details
CVE-2023-3870	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-25180	Rejected reason: Rejected by upstream.	N/A	More Details
CVE-2023-24593	Rejected reason: Rejected by upstream.	N/A	More Details