SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 06 December 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-2023-6269	An argument injection vulnerability has been identified in the administrative web interface of the Atos Unify OpenScape products "Session Border Controller" (SBC) and "Branch", before version V10 R3.4.0, and OpenScape "BCF" before versions V10R10.12.00 and V10R11.05.02. This allows an unauthenticated attacker to gain root access to the appliance via SSH (scope change) and also bypass authentication for the administrative interface and gain access as an arbitrary (administrative) user.	10.0	More Details
CVE-2023-23324	Zumtobel Netlink CCD Onboard 3.74 - Firmware 3.80 was discovered to contain hardcoded credentials for the Administrator account.	9.8	More Details
CVE-2023-48801	In TOTOLINK X6000R_Firmware V9.4.0cu.852_B20230719, the shttpd file sub_415534 function obtains fields from the front-end, connects them through the snprintf function, and passes them to the CsteSystem function, resulting in a command execution vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5952	The Welcart e-Commerce WordPress plugin before 2.9.5 unserializes user input from cookies, which could allow unautehtniacted users to perform PHP Object Injection when a suitable gadget is present on the blog	9.8	More Details
CVE-2023-48967	Ssolon <= 2.6.0 and <=2.5.12 is vulnerable to Deserialization of Untrusted Data.	9.8	More Details
CVE-2023-48910	Microcks up to 1.17.1 was discovered to contain a Server-Side Request Forgery (SSRF) via the component /jobs and /artifact/download. This vulnerability allows attackers to access network resources and sensitive information via a crafted GET request.	9.8	More Details
CVE-2023-48800	In TOTOLINK X6000R_Firmware V9.4.0cu.852_B20230719, the shttpd file sub_417338 function obtains fields from the front-end, connects them through the snprintf function, and passes them to the CsteSystem function, resulting in a command execution vulnerability.	9.8	More Details
CVE-2023-48799	TOTOLINK-X6000R Firmware-V9.4.0cu.852_B20230719 is vulnerable to Command Execution.	9.8	More Details
CVE-2023-49093	HtmlUnit is a GUI-less browser for Java programs. HtmlUnit is vulnerable to Remote Code Execution (RCE) via XSTL, when browsing the attacker’s webpage. This vulnerability has been patched in version 3.9.0	9.8	More Details
CVE-2023-47100	In Perl before 5.38.2, S_parse_uniprop_string in regcomp.c can write to unallocated space because a property name associated with a \p{...} regular expression construct is mishandled. The earliest affected version is 5.30.0.	9.8	More Details
CVE-2023-48887	A deserialization vulnerability in Jupiter v1.3.1 allows attackers to execute arbitrary commands via sending a crafted RPC request.	9.8	More Details
CVE-2023-48886	A deserialization vulnerability in NettyRpc v1.2 allows attackers to execute arbitrary commands via sending a crafted RPC request.	9.8	More Details
CVE-2023-48842	D-Link Go-RT-AC750 revA_v101b03 was discovered to contain a command injection vulnerability via the service parameter at hedwig.cgi.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21163	In PMR_ReadBytes of pmr.c, there is a possible arbitrary code execution due to a use after free. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-49371	RuoYi up to v4.6 was discovered to contain a SQL injection vulnerability via /system/dept/edit.	9.8	More Details
CVE-2023-5636	Unrestricted Upload of File with Dangerous Type vulnerability in ArslanSoft Education Portal allows Command Injection.This issue affects Education Portal: before v1.1.	9.8	More Details
CVE-2023-5634	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ArslanSoft Education Portal allows SQL Injection.This issue affects Education Portal: before v1.1.	9.8	More Details
CVE-2023-43455	An issue in TOTOLINK X6000R V9.4.0cu.652_B20230116 and V9.4.0cu.852_B20230719 allows a remote attacker to execute arbitrary code via the command parameter of the setting/setTracerouteCfg component.	9.8	More Details
CVE-2023-43454	An issue in TOTOLINK X6000R V9.4.0cu.652_B20230116 and V9.4.0cu.852_B20230719 allows a remote attacker to execute arbitrary code via the hostName parameter of the switchOpMode component.	9.8	More Details
CVE-2023-43453	An issue in TOTOLINK X6000R V9.4.0cu.652_B20230116 and V9.4.0cu.852_B20230719 allows a remote attacker to execute arbitrary code via the IP parameter of the setDiagnosisCfg component.	9.8	More Details
CVE-2023-47207	In Delta Electronics InfraSuite Device Master v.1.0.7, a vulnerability exists that allows an unauthenticated attacker to execute code with local administrator privileges.	9.8	More Details
CVE-2023-23325	Zumtobel Netlink CCD Onboard 3.74 - Firmware 3.80 was discovered to contain a command injection vulnerability via the NetHostname parameter.	9.8	More Details
CVE-2023-48812	In TOTOLINK X6000R V9.4.0cu.852_B20230719, the shttpd file sub_4119A0 function obtains fields from the front-end through Uci_ Set_ The Str function that when passed to the CsteSystem function creates a command execution vulnerability.	9.8	More Details
CVE-2023-21162	In RGXUnbackingZSBuffer of rgxta3d.c, there is a possible arbitrary code execution due to a use after free. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21164	In DevmemIntMapPMR of devicemem_server.c, there is a possible arbitrary code execution due to a use after free. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-48810	In TOTOLINK X6000R V9.4.0cu.852_B20230719, the shttpd file, sub_4119A0 function obtains fields from the front-end through Uci_ Set_ The Str function when passed to the CsteSystem function creates a command execution vulnerability.	9.8	More Details
CVE-2023-21166	In RGXBackingZSBuffer of rgxta3d.c, there is a possible arbitrary code execution due to a use after free. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-49070	Pre-auth RCE in Apache Ofbiz 18.12.09. It's due to XML-RPC no longer maintained still present. This issue affects Apache OFBiz: before 18.12.10. Users are recommended to upgrade to version 18.12.10	9.8	More Details
CVE-2023-33083	Memory corruption in WLAN Host while processing RRM beacon on the AP.	9.8	More Details
CVE-2023-33082	Memory corruption while sending an Assoc Request having BTM Query or BTM Response containing MBO IE.	9.8	More Details
CVE-2023-48316	Azure RTOS NetX Duo is a TCP/IP network stack designed specifically for deeply embedded real-time and IoT applications. An attacker can cause remote code execution due to memory overflow vulnerabilities in Azure RTOS NETX Duo. The affected components include processes/functions related to snmp, smtp, ftp and dtls in RTOS v6.2.1 and below. The fixes have been included in NetX Duo release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.8	More Details
CVE-2023-40082	In modify_for_next_stage of fdt.rs, there is a possible way to render KASLR ineffective due to improperly used crypto. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-40078	In a2dp_vendor_opus_decoder_decode_packet of a2dp_vendor_opus_decoder.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to paired device escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35690	In RGXDestroyHWRTData of rgxta3d.c, there is a possible arbitrary code execution due to an uncaught exception. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-24052	An issue discovered in Connectize AC21000 G6 641.139.1.1256 allows attackers to gain control of the device via the change password functionality as it does not prompt for the current password.	9.8	More Details
CVE-2023-24051	A client side rate limit issue discovered in Connectize AC21000 G6 641.139.1.1256 allows attackers to gain escalated privileges via brute force style attacks.	9.8	More Details
CVE-2023-24049	An issue was discovered on Connectize AC21000 G6 641.139.1.1256 allows attackers to gain escalated privileges on the device via poor credential management.	9.8	More Details
CVE-2023-21403	In RGXDestroyZSBufferKM of rgxta3d.c, there is a possible arbitrary code execution due to an uncaught exception. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-21402	In MMU_UnmapPages of mmu_common.c, there is a possible out of bounds read due to improper input validation. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-21401	In DevmemIntChangeSparse of devicemem_server.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-21263	In OSMMapPMRGeneric of pmr_os.c, there is a possible out of bounds write due to an uncaught exception. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-21228	In PMRChangeSparseMemOSMem of physmem_osmem_linux.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21218	In PMRChangeSparseMemOSMem of physmem_osmem_linux.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-21217	In PMRWritePMPageList of TBD, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-21216	In PMRChangeSparseMemOSMem of physmem_osmem_linux.c, there is a possible arbitrary code execution due to a use after free. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-21215	In DevmemIntAcquireRemoteCtx of devicemem_server.c, there is a possible arbitrary code execution due to a race condition. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-48811	In TOTOLINK X6000R V9.4.0cu.852_B20230719, the shttpd file, sub_4119A0 function obtains fields from the front-end through Uci_ Set_ The Str function that when passed to the CsteSystem function creates a command execution vulnerability.	9.8	More Details
CVE-2023-39226	In Delta Electronics InfraSuite Device Master v.1.0.7, a vulnerability exists that allows an unauthenticated attacker to execute arbitrary code through a single UDP packet.	9.8	More Details
CVE-2023-48808	In TOTOLINK X6000R V9.4.0cu.852_B20230719, the shttpd file, sub_4119A0 function obtains fields from the front-end through Uci_ Set_ The Str function when passed to the CsteSystem function creates a command execution vulnerability.	9.8	More Details
CVE-2022-42537	Remote code execution	9.8	More Details
CVE-2023-47463	Insecure Permissions vulnerability in GL.iNet AX1800 version 4.0.0 before 4.5.0 allows a remote attacker to execute arbitrary code via a crafted script to the gl_nas_sys authentication function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48807	In TOTOLINK X6000R V9.4.0cu.852_B20230719, the shttpd file, sub_4119A0 function obtains fields from the front-end through Uci_ Set_ The Str function when passed to the CsteSystem function creates a command execution vulnerability.	9.8	More Details
CVE-2023-4473	A command injection vulnerability in the web server of the Zyxel NAS326 firmware version V5.21(AAZF.14)C0 and NAS542 firmware version V5.21(ABAG.11)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands by sending a crafted URL to a vulnerable device.	9.8	More Details
CVE-2023-35138	A command injection vulnerability in the “show_zysync_server_contents” function of the Zyxel NAS326 firmware version V5.21(AAZF.14)C0 and NAS542 firmware version V5.21(ABAG.11)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands by sending a crafted HTTP POST request.	9.8	More Details
CVE-2023-3741	An OS Command injection vulnerability in NEC Platforms DT900 and DT900S Series all versions allows an attacker to execute any command on the device.	9.8	More Details
CVE-2023-49693	NETGEAR ProSAFE Network Management System has Java Debug Wire Protocol (JDWP) listening on port 11611 and it is remotely accessible by unauthenticated users, allowing attackers to execute arbitrary code.	9.8	More Details
CVE-2022-42541	Remote code execution	9.8	More Details
CVE-2022-42540	Elevation of privilege	9.8	More Details
CVE-2022-42538	Elevation of privilege	9.8	More Details
CVE-2022-42536	Remote code execution	9.8	More Details
CVE-2022-45135	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Cocoon.This issue affects Apache Cocoon: from 2.2.0 before 2.3.0. Users are recommended to upgrade to version 2.3.0, which fixes the issue.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49656	Jenkins MATLAB Plugin 2.11.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	9.8	More Details
CVE-2023-49654	Missing permission checks in Jenkins MATLAB Plugin 2.11.0 and earlier allow attackers to have Jenkins parse an XML file from the Jenkins controller file system.	9.8	More Details
CVE-2023-45484	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the shareSpeed parameter in the function fromSetWifiGuestBasic.	9.8	More Details
CVE-2023-45483	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the time parameter in the function compare_parentcontrol_time.	9.8	More Details
CVE-2023-45482	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the urls parameter in the function get_parentControl_list_Info.	9.8	More Details
CVE-2023-45481	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the firewallEn parameter in the function SetFirewallCfg.	9.8	More Details
CVE-2023-45480	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the src parameter in the function sub_47D878.	9.8	More Details
CVE-2023-45479	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the list parameter in the function sub_49E098.	9.8	More Details
CVE-2023-47462	Insecure Permissions vulnerability in GL.iNet AX1800 v.3.215 and before allows a remote attacker to execute arbitrary code via the file sharing function.	9.8	More Details
CVE-2023-47418	Remote Code Execution (RCE) vulnerability in o2oa version 8.1.2 and before, allows attackers to create a new interface in the service management function to execute JavaScript.	9.8	More Details
CVE-2023-4474	The improper neutralization of special elements in the WSGI server of the Zyxel NAS326 firmware version V5.21(AAZF.14)C0 and NAS542 firmware version V5.21(ABAG.11)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands by sending a crafted URL to a vulnerable device.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49733	Improper Restriction of XML External Entity Reference vulnerability in Apache Cocoon.This issue affects Apache Cocoon: from 2.2.0 before 2.3.0. Users are recommended to upgrade to version 2.3.0, which fixes the issue.	9.8	More Details
CVE-2023-6415	A vulnerability has been reported in Voovi Social Networking Script that affects version 1.0 and consists of a SQL injection via signin.php in the user parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the application.	9.8	More Details
CVE-2023-48806	In TOTOLINK X6000R V9.4.0cu.852_B20230719, the shttpd file, sub_4119A0 function obtains fields from the front-end through Uci_ Set_ The Str function when passed to the CsteSystem function creates a command execution vulnerability.	9.8	More Details
CVE-2023-48805	In TOTOLINK X6000R V9.4.0cu.852_B20230719, the shttpd file, sub_4119A0 function obtains fields from the front-end through Uci_ Set_ The Str function when passed to the CsteSystem function creates a command execution vulnerability.	9.8	More Details
CVE-2023-48804	In TOTOLINK X6000R V9.4.0cu.852_B20230719, the shttpd file, sub_4119A0 function obtains fields from the front-end through Uci_ Set_ The Str function when passed to the CsteSystem function creates a command execution vulnerability.	9.8	More Details
CVE-2023-48803	In TOTOLINK X6000R V9.4.0cu.852_B20230719, the shttpd file, sub_4119A0 function obtains fields from the front-end through Uci_ Set_ The Str function when passed to the CsteSystem function creates a command execution vulnerability.	9.8	More Details
CVE-2023-48802	In TOTOLINK X6000R V9.4.0cu.852_B20230719, the shttpd file, sub_4119A0 function obtains fields from the front-end through Uci_ Set_ The Str function when passed to the CsteSystem function creates a command execution vulnerability.	9.8	More Details
CVE-2023-6418	A vulnerability has been reported in Voovi Social Networking Script that affects version 1.0 and consists of a SQL injection via videos.php in the id parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the application.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6416	A vulnerability has been reported in Voovi Social Networking Script that affects version 1.0 and consists of a SQL injection via signup2.php in the emailadd parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the application.	9.8	More Details
CVE-2023-6417	A vulnerability has been reported in Voovi Social Networking Script that affects version 1.0 and consists of a SQL injection via update.php in the id parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the application.	9.8	More Details
CVE-2023-6448	Unitronics VisiLogic before version 9.9.00, used in Vision and Samba PLCs and HMIs, uses a default administrative password. An unauthenticated attacker with network access can take administrative control of a vulnerable system.	9.8	More Details
CVE-2023-6414	A vulnerability has been reported in Voovi Social Networking Script that affects version 1.0 and consists of a SQL injection via perfil.php in the id and user parameters. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the application.	9.8	More Details
CVE-2023-6026	A Path traversal vulnerability has been reported in elijaa/phpmemcachedadmin affecting version 1.3.0. This vulnerability allows an attacker to delete files stored on the server due to lack of proper verification of user-supplied input.	9.8	More Details
CVE-2023-6413	A vulnerability has been reported in Voovi Social Networking Script that affects version 1.0 and consists of a SQL injection via photos.php in the id and user parameters. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the application.	9.8	More Details
CVE-2023-6410	A vulnerability has been reported in Voovi Social Networking Script that affects version 1.0 and consists of a SQL injection via editprofile.php in multiple parameters. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the application.	9.8	More Details
CVE-2023-6412	A vulnerability has been reported in Voovi Social Networking Script that affects version 1.0 and consists of a SQL injection via photo.php in multiple parameters. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the application.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6411	A vulnerability has been reported in Voovi Social Networking Script that affects version 1.0 and consists of a SQL injection via home.php in the update parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the application.	9.8	More Details
CVE-2023-6345	Integer overflow in Skia in Google Chrome prior to 119.0.6045.199 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a malicious file. (Chromium security severity: High)	9.6	More Details
CVE-2023-49291	tj-actions/branch-names is a Github action to retrieve branch or tag names with support for all events. The `tj-actions/branch-names` GitHub Actions improperly references the `github.event.pull_request.head.ref` and `github.head_ref` context variables within a GitHub Actions `run` step. The head ref variable is the branch name and can be used to execute arbitrary code using a specially crafted branch name. As a result an attacker can use this vulnerability to steal secrets from or abuse `GITHUB_TOKEN` permissions. This vulnerability has been addressed in version 7.0.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.3	More Details
CVE-2023-49079	Misskey is an open source, decentralized social media platform. Misskey's missing signature validation allows arbitrary users to impersonate any remote user. This issue has been patched in version 2023.11.1-beta.1.	9.3	More Details
CVE-2023-49946	In Forgejo before 1.20.5-1, certain endpoints do not check whether an object belongs to a repository for which permissions are being checked. This allows remote attackers to read private issues, read private pull requests, delete issues, and perform other unauthorized actions.	9.1	More Details
CVE-2023-5965	An authenticated privileged attacker could upload a specially crafted zip to the EspoCRM server in version 7.2.5, via the update form, which could lead to arbitrary PHP code execution.	9.1	More Details
CVE-2023-33054	Cryptographic issue in GPS HLOS Driver while downloading Qualcomm GNSS assistance data.	9.1	More Details
CVE-2023-5908	KEPServerEX is vulnerable to a buffer overflow which may allow an attacker to crash the product being accessed or leak information.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5966	An authenticated privileged attacker could upload a specially crafted zip to the EspoCRM server in version 7.2.5, via the extension deployment form, which could lead to arbitrary PHP code execution.	9.1	More Details
CVE-2023-46886	Dreamer CMS before version 4.0.1 is vulnerable to Directory Traversal. Background template management allows arbitrary modification of the template file, allowing system sensitive files to be read.	9.1	More Details
CVE-2023-44382	October is a Content Management System (CMS) and web platform to assist with development workflow. An authenticated backend user with the \`editor.cms_pages\`, \`editor.cms_layouts\`, or \`editor.cms_partials\` permissions who would normally not be permitted to provide PHP code to be executed by the CMS due to \`cms.safe_mode\` being enabled can write specific Twig code to escape the Twig sandbox and execute arbitrary PHP. This issue has been patched in 3.4.15.	9.1	More Details
CVE-2023-48692	Azure RTOS NetX Duo is a TCP/IP network stack designed specifically for deeply embedded real-time and IoT applications. An attacker can cause remote code execution due to memory overflow vulnerabilities in Azure RTOS NETX Duo. The affected components include processes/functions related to icmp, tcp, snmp, dhcp, nat and ftp in RTOS v6.2.1 and below. The fixes have been included in NetX Duo release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-48912	Dreamer CMS v4.1.3 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/archives/edit.	8.8	More Details
CVE-2023-24048	Cross Site Request Forgery (CSRF) vulnerability in Connectize AC21000 G6 641.139.1.1256 allows attackers to gain control of the device via crafted GET request to /man_password.htm.	8.8	More Details
CVE-2023-49381	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/div/update.	8.8	More Details
CVE-2023-49382	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/div/delete.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49383	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/tag/save.	8.8	More Details
CVE-2023-40088	In callback_thread_event of com_android_bluetooth_btservice_AdapterService.cpp, there is a possible memory corruption due to a use after free. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2023-40087	In transcodeQ*ToFloat of btif_avrcp_audio_track.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to paired device escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2023-49395	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/category/update.	8.8	More Details
CVE-2023-49052	File Upload vulnerability in Microweber v.2.0.4 allows a remote attacker to execute arbitrary code via a crafted script to the file upload function in the created forms component.	8.8	More Details
CVE-2023-37927	The improper neutralization of special elements in the CGI program of the Zyxel NAS326 firmware version V5.21(AAZF.14)C0 and NAS542 firmware version V5.21(ABAG.11)C0 could allow an authenticated attacker to execute some operating system (OS) commands by sending a crafted URL to a vulnerable device.	8.8	More Details
CVE-2023-49396	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/category/save.	8.8	More Details
CVE-2023-49397	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/category/updateStatus.	8.8	More Details
CVE-2023-49398	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/category/delete.	8.8	More Details
CVE-2023-49446	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/nav/save.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47464	Insecure Permissions vulnerability in GL.iNet AX1800 version 4.0.0 before 4.5.0 allows a remote attacker to execute arbitrary code via the upload API function.	8.8	More Details
CVE-2023-49447	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/nav/update.	8.8	More Details
CVE-2023-49380	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/friend_link/delete.	8.8	More Details
CVE-2023-49379	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via the component /admin/friend_link/save.	8.8	More Details
CVE-2023-49378	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/form/save.	8.8	More Details
CVE-2023-49377	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/tag/update.	8.8	More Details
CVE-2023-49376	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/tag/delete.	8.8	More Details
CVE-2023-49375	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/friend_link/update.	8.8	More Details
CVE-2023-49374	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/slide/update.	8.8	More Details
CVE-2023-49373	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via /admin/slide/delete.	8.8	More Details
CVE-2023-49372	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/slide/save.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48913	Dreamer CMS v4.1.3 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/archives/delete.	8.8	More Details
CVE-2023-48914	Dreamer CMS v4.1.3 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/archives/add.	8.8	More Details
CVE-2023-48315	Azure RTOS NetX Duo is a TCP/IP network stack designed specifically for deeply embedded real-time and IoT applications. An attacker can cause remote code execution due to memory overflow vulnerabilities in Azure RTOS NETX Duo. The affected components include processes/functions related to ftp and sntp in RTOS v6.2.1 and below. The fixes have been included in NetX Duo release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2022-47531	An issue was discovered in Ericsson Evolved Packet Gateway (EPG) versions 3.x before 3.25 and 2.x before 2.16, allows authenticated users to bypass system CLI and execute commands they are authorized to execute directly in the UNIX shell.	8.8	More Details
CVE-2023-48893	SLiMS (aka SENAYAN Library Management System) through 9.6.1 allows admin/modules/reporting/customs/staff_act.php SQL Injection via startDate or untilDate.	8.8	More Details
CVE-2023-48813	Senayan Library Management Systems (Slims) 9 Bulian v9.6.1 is vulnerable to SQL Injection via admin/modules/reporting/customs/fines_report.php.	8.8	More Details
CVE-2023-46326	ZStack Cloud version 3.10.38 and before allows unauthenticated API access to the list of active job UUIDs and the session ID for each of these. This leads to privilege escalation.	8.8	More Details
CVE-2023-42917	A memory corruption vulnerability was addressed with improved locking. This issue is fixed in iOS 17.1.2 and iPadOS 17.1.2, macOS Sonoma 14.1.2, Safari 17.1.2. Processing web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited against versions of iOS before iOS 16.7.1.	8.8	More Details
CVE-2023-37928	A post-authentication command injection vulnerability in the WSGI server of the Zyxel NAS326 firmware version V5.21(AAZF.14)C0 and NAS542 firmware version V5.21(ABAG.11)C0 could allow an authenticated attacker to execute some operating system (OS) commands by sending a crafted URL to a vulnerable device.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46690	In Delta Electronics InfraSuite Device Master v.1.0.7, a vulnerability exists that allows an attacker to write to any file to any location of the filesystem, which could lead to remote code execution.	8.8	More Details
CVE-2023-5953	The Welcart e-Commerce WordPress plugin before 2.9.5 does not validate files to be uploaded, as well as does not have authorisation and CSRF in an AJAX action handling such upload. As a result, any authenticated users, such as subscriber could upload arbitrary files, such as PHP on the server	8.8	More Details
CVE-2023-6357	A low-privileged remote attacker could exploit the vulnerability and inject additional system commands via file system libraries which could give the attacker full control of the device.	8.8	More Details
CVE-2023-48966	An arbitrary file upload vulnerability in the component /admin/api.upload/file of ThinkAdmin v6.1.53 allows attackers to execute arbitrary code via a crafted Zip file.	8.8	More Details
CVE-2023-6348	Type Confusion in Spellcheck in Google Chrome prior to 119.0.6045.199 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-5762	The Filr WordPress plugin before 1.2.3.6 is vulnerable from an RCE (Remote Code Execution) vulnerability, which allows the operating system to execute commands and fully compromise the server on behalf of a user with Author-level privileges.	8.8	More Details
CVE-2023-6350	Use after free in libavif in Google Chrome prior to 119.0.6045.199 allowed a remote attacker to potentially exploit heap corruption via a crafted avif file. (Chromium security severity: High)	8.8	More Details
CVE-2023-49673	A cross-site request forgery (CSRF) vulnerability in Jenkins NeuVector Vulnerability Scanner Plugin 1.22 and earlier allows attackers to connect to an attacker-specified hostname and port using attacker-specified username and password.	8.8	More Details
CVE-2023-49108	Path traversal vulnerability exists in RakRak Document Plus Ver.3.2.0.0 to Ver.6.4.0.7 (excluding Ver.6.1.1.3a). If this vulnerability is exploited, arbitrary files on the server may be obtained or deleted by a user of the product with specific privileges.	8.8	More Details
CVE-2023-6347	Use after free in Mojo in Google Chrome prior to 119.0.6045.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6346	Use after free in WebAudio in Google Chrome prior to 119.0.6045.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-44304	Dell DM5500 contains a privilege escalation vulnerability in the appliance. A remote attacker with low privileges could potentially exploit this vulnerability to escape the restricted shell and gain root access to the appliance.	8.8	More Details
CVE-2023-6351	Use after free in libavif in Google Chrome prior to 119.0.6045.199 allowed a remote attacker to potentially exploit heap corruption via a crafted avif file. (Chromium security severity: High)	8.8	More Details
CVE-2023-49655	A cross-site request forgery (CSRF) vulnerability in Jenkins MATLAB Plugin 2.11.0 and earlier allows attackers to have Jenkins parse an XML file from the Jenkins controller file system.	8.8	More Details
CVE-2023-49448	JFinalCMS v5.0.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via admin/nav/delete.	8.8	More Details
CVE-2023-49091	Cosmos provides users the ability self-host a home server by acting as a secure gateway to your application, as well as a server manager. Cosmos-server is vulnerable due to to the authorization header used for user login remaining valid and not expiring after log out. This vulnerability allows an attacker to use the token to gain unauthorized access to the application/system even after the user has logged out. This issue has been patched in version 0.13.0.	8.8	More Details
CVE-2023-48965	An issue in the component /admin/api.plugs/script of ThinkAdmin v6.1.53 allows attackers to getshell via providing a crafted URL to download a malicious PHP file.	8.8	More Details
CVE-2023-5970	Improper authentication in the SMA100 SSL-VPN virtual office portal allows a remote authenticated attacker to create an identical external domain user using accent characters, resulting in an MFA bypass.	8.8	More Details
CVE-2023-48693	Azure RTOS ThreadX is an advanced real-time operating system (RTOS) designed specifically for deeply embedded applications. An attacker can cause arbitrary read and write due to vulnerability in parameter checking mechanism in Azure RTOS ThreadX, which may lead to privilege escalation. The affected components include RTOS ThreadX v6.2.1 and below. The fixes have been included in ThreadX release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6033	Improper neutralization of input in Jira integration configuration in GitLab CE/EE, affecting all versions from 15.10 prior to 16.6.1, 16.5 prior to 16.5.3, and 16.4 prior to 16.4.3 allows attacker to execute javascript in victim's browser.	8.7	More Details
CVE-2023-49286	Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. Due to an Incorrect Check of Function Return Value bug Squid is vulnerable to a Denial of Service attack against its Helper process management. This bug is fixed by Squid version 6.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.6	More Details
CVE-2023-49285	Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. Due to a Buffer Overread bug Squid is vulnerable to a Denial of Service attack against Squid HTTP Message processing. This bug is fixed by Squid version 6.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.6	More Details
CVE-2023-49095	nexkey is a microblogging platform. Insufficient validation of ActivityPub requests received in inbox could allow any user to impersonate another user in certain circumstances. This issue has been patched in version 12.122.2.	8.6	More Details
CVE-2023-6360	The 'My Calendar' WordPress Plugin, version < 3.4.22 is affected by an unauthenticated SQL injection vulnerability in the 'from' and 'to' parameters in the '/my-calendar/v1/events' rest route.	8.6	More Details
CVE-2023-49288	Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. Affected versions of squid are subject to a a Use-After-Free bug which can lead to a Denial of Service attack via collapsed forwarding. All versions of Squid from 3.5 up to and including 5.9 configured with "collapsed_forwarding on" are vulnerable. Configurations with "collapsed_forwarding off" or without a "collapsed_forwarding" directive are not vulnerable. This bug is fixed by Squid version 6.0.1. Users are advised to upgrade. Users unable to upgrade should remove all collapsed_forwarding lines from their squid.conf.	8.6	More Details
CVE-2023-42006	IBM Administration Runtime Expert for i 7.2, 7.3, 7.4, and 7.5 could allow a local user to obtain sensitive information caused by improper authority checks. IBM X-Force ID: 265266.	8.4	More Details
CVE-2023-33022	Memory corruption in HLOS while invoking IOCTL calls from user-space.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45168	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the invscout command to execute arbitrary commands. IBM X-Force ID: 267966.	8.4	More Details
CVE-2023-33053	Memory corruption in Kernel while parsing metadata.	8.4	More Details
CVE-2023-33071	Memory corruption in Automotive OS whenever untrusted apps try to access HAb for graphics functionalities.	8.4	More Details
CVE-2023-33088	Memory corruption when processing cmd parameters while parsing vdev.	8.4	More Details
CVE-2023-33092	Memory corruption while processing pin reply in Bluetooth, when pin code received from APP layer is greater than expected size.	8.4	More Details
CVE-2023-33107	Memory corruption in Graphics Linux while assigning shared virtual memory region during IOCTL call.	8.4	More Details
CVE-2023-33106	Memory corruption while submitting a large list of sync points in an AUX command to the IOCTL_KGSL_GPU_AUX_COMMAND.	8.4	More Details
CVE-2023-6071	An Improper Neutralization of Special Elements used in a command vulnerability in ESM prior to version 11.6.9 allows a remote administrator to execute arbitrary code as root on the ESM. This is possible as the input isn't correctly sanitized when adding a new data source.	8.4	More Details
CVE-2023-49077	Mailcow: dockerized is an open source groupware/email suite based on docker. A Cross-Site Scripting (XSS) vulnerability has been identified within the Quarantine UI of the system. This vulnerability poses a significant threat to administrators who utilize the Quarantine feature. An attacker can send a carefully crafted email containing malicious JavaScript code. This issue has been patched in version 2023-11.	8.3	More Details
CVE-2023-40465	Several versions of ALEOS, including ALEOS 4.16.0, include an opensource third-party component which can be exploited from the local area network, resulting in a Denial of Service condition for the captive portal.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49277	dpaste is an open source pastebin application written in Python using the Django framework. A security vulnerability has been identified in the expires parameter of the dpaste API, allowing for a POST Reflected XSS attack. This vulnerability can be exploited by an attacker to execute arbitrary JavaScript code in the context of a user's browser, potentially leading to unauthorized access, data theft, or other malicious activities. Users are strongly advised to upgrade to dpaste release v3.8 or later versions, as dpaste versions older than v3.8 are susceptible to the identified security vulnerability. No known workarounds have been identified, and applying the patch is the most effective way to remediate the vulnerability.	8.3	More Details
CVE-2023-28585	Memory corruption while loading an ELF segment in TEE Kernel.	8.2	More Details
CVE-2023-45841	Multiple data integrity vulnerabilities exist in the package hash checking functionality of Buildroot 2023.08.1 and Buildroot dev commit 622698d7847. A specially crafted man-in-the-middle attack can lead to arbitrary command execution in the builder.This vulnerability is related to the `versal-firmware` package.	8.1	More Details
CVE-2023-45838	Multiple data integrity vulnerabilities exist in the package hash checking functionality of Buildroot 2023.08.1 and Buildroot dev commit 622698d7847. A specially crafted man-in-the-middle attack can lead to arbitrary command execution in the builder.This vulnerability is related to the `aufs` package.	8.1	More Details
CVE-2023-40461	The ACEManager component of ALEOS 4.16 and earlier allows an authenticated user with Administrator privileges to access a file upload field which does not fully validate the file name, creating a Stored Cross-Site Scripting condition.	8.1	More Details
CVE-2023-48691	Azure RTOS NetX Duo is a TCP/IP network stack designed specifically for deeply embedded real-time and IoT applications. An attacker can cause an out-of-bounds write in Azure RTOS NETX Duo, that could lead to remote code execution. The affected components include process related to IGMP protocol in RTOS v6.2.1 and below. The fix has been included in NetX Duo release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.1	More Details
CVE-2022-46480	Incorrect Session Management and Credential Re-use in the Bluetooth LE stack of the Ultraloq UL3 2nd Gen Smart Lock Firmware 02.27.0012 allows an attacker to sniff the unlock code and unlock the device whilst within Bluetooth range.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45839	Multiple data integrity vulnerabilities exist in the package hash checking functionality of Buildroot 2023.08.1 and Buildroot dev commit 622698d7847. A specially crafted man-in-the-middle attack can lead to arbitrary command execution in the builder.This vulnerability is related to the `aufs-util` package.	8.1	More Details
CVE-2023-45840	Multiple data integrity vulnerabilities exist in the package hash checking functionality of Buildroot 2023.08.1 and Buildroot dev commit 622698d7847. A specially crafted man-in-the-middle attack can lead to arbitrary command execution in the builder.This vulnerability is related to the `riscv64-elf-toolchain` package.	8.1	More Details
CVE-2023-44305	Dell DM5500 5.14.0.0, contains a Stack-based Buffer Overflow Vulnerability in the appliance. An unauthenticated remote attacker may exploit this vulnerability to crash the affected process or execute arbitrary code on the system by sending specially crafted input data.	8.1	More Details
CVE-2023-40077	In multiple functions of MetaDataBase.cpp, there is a possible UAF write due to a race condition. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.1	More Details
CVE-2023-44302	Dell DM5500 5.14.0.0 and prior contain an improper authentication vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability to gain access of resources or functionality that could possibly lead to execute arbitrary code.	8.1	More Details
CVE-2023-43608	A data integrity vulnerability exists in the BR_NO_CHECK_HASH_FOR functionality of Buildroot 2023.08.1 and dev commit 622698d7847. A specially crafted man-in-the-middle attack can lead to arbitrary command execution in the builder.	8.1	More Details
CVE-2023-40463	When configured in debugging mode by an authenticated user with administrative privileges, ALEOS 4.16 and earlier store the SHA512 hash of the common root password for that version in a directory accessible to a user with root privileges or equivalent access.	8.1	More Details
CVE-2023-40464	Several versions of ALEOS, including ALEOS 4.16.0, use a hardcoded SSL certificate and private key. An attacker with access to these items could potentially perform a man in the middle attack between the ACEManager client and ACEManager server.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45842	Multiple data integrity vulnerabilities exist in the package hash checking functionality of Buildroot 2023.08.1 and Buildroot dev commit 622698d7847. A specially crafted man-in-the-middle attack can lead to arbitrary command execution in the builder.This vulnerability is related to the `mxsldr` package.	8.1	More Details
CVE-2023-49097	ZITADEL is an identity infrastructure system. ZITADEL uses the notification triggering requests Forwarded or X-Forwarded-Host header to build the button link sent in emails for confirming a password reset with the emailed code. If this header is overwritten and a user clicks the link to a malicious site in the email, the secret code can be retrieved and used to reset the users password and take over his account. Accounts with MFA or Passwordless enabled can not be taken over by this attack. This issue has been patched in versions 2.41.6, 2.40.10 and 2.39.9.	8.1	More Details
CVE-2023-42690	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-42691	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-42685	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-42689	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-42687	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-5944	Delta Electronics DOPSoft is vulnerable to a stack-based buffer overflow, which may allow for arbitrary code execution if an attacker can lead a legitimate user to execute a specially crafted file.	7.8	More Details
CVE-2023-42686	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-42688	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49694	A low-privileged OS user with access to a Windows host where NETGEAR ProSAFE Network Management System is installed can create arbitrary JSP files in a Tomcat web application directory. The user can then execute the JSP files under the security context of SYSTEM.	7.8	More Details
CVE-2023-42681	In ion service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-33063	Memory corruption in DSP Services during a remote call from HLOS to DSP.	7.8	More Details
CVE-2023-47454	An Untrusted search path vulnerability in NetEase CloudMusic 2.10.4 for Windows allows local users to gain escalated privileges through the urlmon.dll file in the current working directory.	7.8	More Details
CVE-2023-47453	An Untrusted search path vulnerability in Sohu Video Player 7.0.15.0 allows local users to gain escalated privileges through the version.dll file in the current working directory.	7.8	More Details
CVE-2023-47452	An Untrusted search path vulnerability in notepad++ 6.5 allows local users to gain escalated privileges through the msimg32.dll file in the current working directory.	7.8	More Details
CVE-2023-45252	DLL Hijacking vulnerability in Huddly HuddlyCameraService before version 8.0.7, not including version 7.99, due to the installation of the service in a directory that grants write privileges to standard users, allows attackers to manipulate files, execute arbitrary code, and escalate privileges.	7.8	More Details
CVE-2023-45253	An issue was discovered in Huddly HuddlyCameraService before version 8.0.7, not including version 7.99, allows attackers to manipulate files and escalate privileges via RollingFileAppender.DeleteFile method performed by the log4net library.	7.8	More Details
CVE-2023-33087	Memory corruption in Core while processing RX intent request.	7.8	More Details
CVE-2023-33079	Memory corruption in Audio while running invalid audio recording from ADSP.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5427	Use After Free vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user to make improper GPU processing operations to gain access to already freed memory.This issue affects Bifrost GPU Kernel Driver: from r44p0 through r45p0; Valhall GPU Kernel Driver: from r44p0 through r45p0; Arm 5th Gen GPU Architecture Kernel Driver: from r44p0 through r45p0.	7.8	More Details
CVE-2023-28546	Memory Corruption in SPS Application while exporting public key in sorter TA.	7.8	More Details
CVE-2023-33018	Memory corruption while using the UIM diag command to get the operators name.	7.8	More Details
CVE-2023-47304	An issue was discovered in Vonage Box Telephone Adapter VDV23 version VDV21-3.2.11-0.5.1, allows local attackers to bypass UART authentication controls and read/write arbitrary values to the memory of the device.	7.8	More Details
CVE-2023-33017	Memory corruption in Boot while running a ListVars test in UEFI Menu during boot.	7.8	More Details
CVE-2023-28587	Memory corruption in BT controller while parsing debug commands with specific sub-opcodes at HCI interface level.	7.8	More Details
CVE-2023-42693	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-28551	Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments.	7.8	More Details
CVE-2023-28550	Memory corruption in MPP performance while accessing DSM watermark using external memory address.	7.8	More Details
CVE-2023-42692	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42695	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-42694	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-40097	In hasPermissionForActivity of PackageManagerHelper.java, there is a possible URI grant due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2023-42743	In telecom service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-32804	Out-of-bounds Write vulnerability in Arm Ltd Midgard GPU Userspace Driver, Arm Ltd Bifrost GPU Userspace Driver, Arm Ltd Valhall GPU Userspace Driver, Arm Ltd Arm 5th Gen GPU Architecture Userspace Driver allows a local non-privileged user to write a constant pattern to a limited amount of memory not allocated by the user space driver.This issue affects Midgard GPU Userspace Driver: from r0p0 through r32p0; Bifrost GPU Userspace Driver: from r0p0 through r44p0; Valhall GPU Userspace Driver: from r19p0 through r44p0; Arm 5th Gen GPU Architecture Userspace Driver: from r41p0 through r44p0.	7.8	More Details
CVE-2023-40103	In multiple locations, there is a possible way to corrupt memory due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-42740	In telecom service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-42739	In engineermode service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-42738	In telocom service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40096	In OpRecordAudioMonitor::onFirstRef of AudioRecordClient.cpp, there is a possible way to record audio from the background due to a missing flag. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-40080	In multiple functions of btm_ble_gap.cc, there is a possible out of bounds write due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-40095	In createDontSendToRestrictedAppsBundle of PendingIntentUtils.java, there is a possible background activity launch due to a missing check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-40094	In keyguardGoingAway of ActivityTaskManagerService.java, there is a possible lock screen bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-40091	In onTransact of IncidentService.cpp, there is a possible out of bounds write due to memory corruption. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-40089	In getCredentialManagerPolicy of DevicePolicyManagerService.java, there is a possible method for users to select credential managers without permission due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-40084	In run of MDnsSdListener.cpp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-42736	In telecom service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-42745	In telecom service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42746	In power manager, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-42747	In camera service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-42748	In telecom service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-42696	In telecom service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-5247	Malicious Code Execution Vulnerability due to External Control of File Name or Path in multiple Mitsubishi Electric FA Engineering Software Products allows a malicious attacker to execute a malicious code by having legitimate users open a specially crafted project file, which could result in information disclosure, tampering and deletion, or a denial-of-service (DoS) condition.	7.8	More Details
CVE-2023-45779	In the APEX module framework of AOSP, there is a possible malicious update to platform components due to improperly used crypto. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. More details on this can be found in the referenced links.	7.8	More Details
CVE-2023-45777	In checkKeyIntentParceledCorrectly of AccountManagerService.java, there is a possible way to launch arbitrary activities using system privileges due to Parcel Mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-45776	In CreateAudioBroadcast of broadcaster.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-45775	In CreateAudioBroadcast of broadcaster.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45774	In fixUpIncomingShortcutInfo of ShortcutService.java, there is a possible way to view another user's image due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-45773	In multiple functions of btm_ble_gap.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-32847	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS08241940; Issue ID: ALPS08241940.	7.8	More Details
CVE-2023-32850	In decoder, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS08016659; Issue ID: ALPS08016659.	7.8	More Details
CVE-2023-32851	In decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS08016652; Issue ID: ALPS08016652.	7.8	More Details
CVE-2023-41613	EzViz Studio v2.2.0 is vulnerable to DLL hijacking.	7.8	More Details
CVE-2023-40079	In injectSendIntentSender of ShortcutService.java, there is a possible background activity launch due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49280	XWiki Change Request is an XWiki application allowing to request changes on a wiki without publishing directly the changes. Change request allows to edit any page by default, and the changes are then exported in an XML file that anyone can download. So it's possible for an attacker to obtain password hash of users by performing an edit on the user profiles and then downloading the XML file that has been created. This is also true for any document that might contain password field and that a user can view. This vulnerability impacts all version of Change Request, but the impact depends on the rights that has been set on the wiki since it requires for the user to have the Change request right (allowed by default) and view rights on the page to target. This issue cannot be easily exploited in an automated way. The patch consists in denying to users the right of editing pages that contains a password field with change request. It means that already existing change request for those pages won't be removed by the patch, administrators needs to take care of it. The patch is provided in Change Request 1.10, administrators should upgrade immediately. It's possible to workaround the vulnerability by denying manually the Change request right on some spaces, such as XWiki space which will include any user profile by default.	7.7	More Details
CVE-2023-49287	TinyDir is a lightweight C directory and file reader. Buffer overflows in the \`tinydir_file_open()\` function. This vulnerability has been patched in version 1.2.6.	7.7	More Details
CVE-2023-42571	Abuse of remote unlock in Find My Mobile prior to version 7.3.13.4 allows physical attacker to unlock the device remotely by resetting the Samsung Account password with SMS verification when user lost the device.	7.6	More Details
CVE-2023-48742	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LicenseManager License Manager for WooCommerce license-manager-for-woocommerce allows SQL Injection.This issue affects License Manager for WooCommerce: from n/a through 2.2.10.	7.6	More Details
CVE-2023-5808	SMU versions prior to 14.8.7825.01 are susceptible to unintended information disclosure, through URL manipulation. Authenticated users in a Storage administrative role are able to access HNAS configuration backup and diagnostic data, that would normally be barred to that specific administrative role.	7.6	More Details
CVE-2023-46384	LOYTEC electronics GmbH LINX Configurator (all versions) is vulnerable to Insecure Permissions. Cleartext storage of credentials allows remote attackers to disclose admin password and bypass an authentication to login Loytec device.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21227	In HTBLogKM of htbserver.c, there is a possible information disclosure due to log information disclosure. This could lead to local information disclosure in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2023-47307	Buffer Overflow vulnerability in /apply.cgi in Shenzhen Libituo Technology Co., Ltd LBT-T300-T310 v2.2.2.6 allows attackers to cause a denial of service via the ApCliAuthMode parameter.	7.5	More Details
CVE-2023-46389	LOYTEC electronics GmbH LINX-212 and LINX-151 devices (all versions) are vulnerable to Incorrect Access Control via registry.xml file. This vulnerability allows remote attackers to disclose sensitive information on LINX configuration.	7.5	More Details
CVE-2023-46388	LOYTEC electronics GmbH LINX-212 and LINX-151 devices (all versions) are vulnerable to Insecure Permissions via dpal_config.zml file. This vulnerability allows remote attackers to disclose smtp client account credentials and bypass email authentication.	7.5	More Details
CVE-2023-46387	LOYTEC electronics GmbH LINX-212 and LINX-151 devices (all versions) are vulnerable to Incorrect Access Control via dpal_config.zml file. This vulnerability allows remote attackers to disclose sensitive information on Loytec device data point configuration.	7.5	More Details
CVE-2023-46386	LOYTEC electronics GmbH LINX-212 and LINX-151 devices (all versions) are vulnerable to Insecure Permissions via registry.xml file. This vulnerability allows remote attackers to disclose smtp client account credentials and bypass email authentication.	7.5	More Details
CVE-2023-46385	LOYTEC electronics GmbH LINX Configurator (all versions) is vulnerable to Insecure Permissions. An admin credential is passed as a value of URL parameters without encryption, so it allows remote attackers to steal the password and gain full control of Loytec device configuration.	7.5	More Details
CVE-2023-46383	LOYTEC electronics GmbH LINX Configurator (all versions) uses HTTP Basic Authentication, which transmits usernames and passwords in base64-encoded cleartext and allows remote attackers to steal the password and gain full control of Loytec device configuration.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49735	** UNSUPPORTED WHEN ASSIGNED ** The value set as the DefaultLocaleResolver.LOCALE_KEY attribute on the session was not validated while resolving XML definition files, leading to possible path traversal and eventually SSRF/XXE when passing user-controlled data to this key. Passing user-controlled data to this key may be relatively common, as it was also used like that to set the language in the 'tiles-test' application shipped with Tiles. This issue affects Apache Tiles from version 2 onwards. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	7.5	More Details
CVE-2023-47633	Traefik is an open source HTTP reverse proxy and load balancer. The traefik docker container uses 100% CPU when it serves as its own backend, which is an automatically generated route resulting from the Docker integration in the default configuration. This issue has been addressed in versions 2.10.6 and 3.0.0-beta5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2023-32846	In 5G Modem, there is a possible system crash due to improper error handling. This could lead to remote denial of service when receiving malformed RRC messages, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01128524; Issue ID: MOLY01138453 (MSV-861).	7.5	More Details
CVE-2023-32845	In 5G Modem, there is a possible system crash due to improper error handling. This could lead to remote denial of service when receiving malformed RRC messages, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01128524; Issue ID: MOLY01139296 (MSV-860).	7.5	More Details
CVE-2023-32844	In 5G Modem, there is a possible system crash due to improper error handling. This could lead to remote denial of service when receiving malformed RRC messages, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01128524; Issue ID: MOLY01130183 (MSV-850).	7.5	More Details
CVE-2023-46887	In Dreamer CMS before 4.0.1, the backend attachment management office has an Arbitrary File Download vulnerability.	7.5	More Details
CVE-2023-32843	In 5G Modem, there is a possible system crash due to improper error handling. This could lead to remote denial of service when receiving malformed RRC messages, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01130204; Issue ID: MOLY01130204 (MSV-849).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32842	In 5G Modem, there is a possible system crash due to improper error handling. This could lead to remote denial of service when receiving malformed RRC messages, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01130256; Issue ID: MOLY01130256 (MSV-848).	7.5	More Details
CVE-2023-5909	KEPServerEX does not properly validate certificates from clients which may allow unauthenticated users to connect.	7.5	More Details
CVE-2023-48016	Restaurant Table Booking System V1.0 is vulnerable to SQL Injection in rtbs/admin/index.php via the username parameter.	7.5	More Details
CVE-2023-33043	Transient DOS in Modem when a Beam switch request is made with a non-configured BWP.	7.5	More Details
CVE-2023-33042	Transient DOS in Modem after RRC Setup message is received.	7.5	More Details
CVE-2023-42717	In telephony service, there is a possible missing permission check. This could lead to remote information disclosure no additional execution privileges needed	7.5	More Details
CVE-2023-32841	In 5G Modem, there is a possible system crash due to improper error handling. This could lead to remote denial of service when receiving malformed RRC messages, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01128524; Issue ID: MOLY01128524 (MSV-846).	7.5	More Details
CVE-2023-40699	IBM InfoSphere Information Server 11.7 could allow a remote attacker to cause a denial of service due to improper input validation. IBM X-Force ID: 265161.	7.5	More Details
CVE-2023-33041	Under certain scenarios the WLAN Firmware will reach an assertion due to state confusion while looking up peer ids.	7.5	More Details
CVE-2023-28588	Transient DOS in Bluetooth Host while rfc slot allocation.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5637	Unrestricted Upload of File with Dangerous Type vulnerability in ArslanSoft Education Portal allows Read Sensitive Strings Within an Executable.This issue affects Education Portal: before v1.1.	7.5	More Details
CVE-2023-5635	Improper Protection for Outbound Error Messages and Alert Signals vulnerability in ArslanSoft Education Portal allows Account Footprinting.This issue affects Education Portal: before v1.1.	7.5	More Details
CVE-2023-33044	Transient DOS in Data modem while handling TLB control messages from the Network.	7.5	More Details
CVE-2023-42716	In telephony service, there is a possible missing permission check. This could lead to remote information disclosure no additional execution privileges needed	7.5	More Details
CVE-2023-33089	Transient DOS when processing a NULL buffer while parsing WLAN vdev.	7.5	More Details
CVE-2023-49947	Forgejo before 1.20.5-1 allows 2FA bypass when docker login uses Basic Authentication.	7.5	More Details
CVE-2023-6063	The WP Fastest Cache WordPress plugin before 1.2.2 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by unauthenticated users.	7.5	More Details
CVE-2023-48863	SEMCMS 3.9 is vulnerable to SQL Injection. Due to the lack of security checks on the input of the application, the attacker uses the existing application to inject malicious SQL commands into the background database engine for execution, and sends some attack codes as commands or query statements to the interpreter. These malicious data can deceive the interpreter, so as to execute unplanned commands or unauthorized access to data.	7.5	More Details
CVE-2023-40459	The ACEManager component of ALEOS 4.16 and earlier does not adequately perform input sanitization during authentication, which could potentially result in a Denial of Service (DoS) condition for ACEManager without impairing other router functions. ACEManager recovers from the DoS condition by restarting within ten seconds of becoming unavailable.	7.5	More Details
CVE-2023-33080	Transient DOS while parsing a vender specific IE (Information Element) of reassociation response management frame.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33081	Transient DOS while converting TWT (Target Wake Time) frame parameters in the OTA broadcast.	7.5	More Details
CVE-2023-40462	The ACEManager component of ALEOS 4.16 and earlier does not perform input sanitization during authentication, which could potentially result in a Denial of Service (DoS) condition for ACEManager without impairing other router functions. ACEManager recovers from the DoS condition by restarting within ten seconds of becoming unavailable.	7.5	More Details
CVE-2023-24294	Zumtobel Netlink CCD Onboard v3.74 - Firmware v3.80 was discovered to contain a buffer overflow via the component NetlinkWeb::Information::SetDeviceIdentification.	7.5	More Details
CVE-2023-47279	In Delta Electronics InfraSuite Device Master v.1.0.7, A vulnerability exists that allows an unauthenticated attacker to disclose user information through a single UDP packet, obtain plaintext credentials, or perform NTLM relaying.	7.5	More Details
CVE-2022-42539	Information disclosure	7.5	More Details
CVE-2023-5188	The MMS Interpreter of WagoAppRTU in versions below 1.4.6.0 which is used by the WAGO Telecontrol Configurator is vulnerable to malformed packets. An remote unauthenticated attacker could send specifically crafted packets that lead to a denial-of-service condition until restart of the affected device.	7.5	More Details
CVE-2023-48952	An issue in the box_deserialize_reusing function in openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) after running a SELECT statement.	7.5	More Details
CVE-2023-41835	When a Multipart request is performed but some of the fields exceed the maxStringLength limit, the upload files will remain in struts.multipart.saveDir even if the request has been denied. Users are recommended to upgrade to versions Struts 2.5.32 or 6.1.2.2 or Struts 6.3.0.1 or greater, which fixe this issue.	7.5	More Details
CVE-2023-44288	Dell PowerScale OneFS, 8.2.2.x through 9.6.0.x, contains an improper control of a resource through its lifetime vulnerability. An unauthenticated network attacker could potentially exploit this vulnerability, leading to denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40458	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in Sierra Wireless, Inc ALEOS could potentially allow a remote attacker to trigger a Denial of Service (DoS) condition for ACEManager without impairing other router functions. This condition is cleared by restarting the device.	7.5	More Details
CVE-2023-44150	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in ProfilePress Membership Team Paid Membership Plugin, Ecommerce, Registration Form, Login Form, User Profile & Restrict Content – ProfilePress.This issue affects Paid Membership Plugin, Ecommerce, Registration Form, Login Form, User Profile & Restrict Content – ProfilePress: from n/a through 4.13.2.	7.5	More Details
CVE-2023-35137	An improper authentication vulnerability in the authentication module of the Zyxel NAS326 firmware version V5.21(AAZF.14)C0 and NAS542 firmware version V5.21(ABAG.11)C0 could allow an unauthenticated attacker to obtain system information by sending a crafted URL to a vulnerable device.	7.5	More Details
CVE-2023-40600	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Exactly WWW EWWW Image Optimizer. It works only when debug.log is turned on.This issue affects EWWW Image Optimizer: from n/a through 7.2.0.	7.5	More Details
CVE-2023-45287	Before Go 1.20, the RSA based TLS key exchanges used the math/big library, which is not constant time. RSA blinding was applied to prevent timing attacks, but analysis shows this may not have been fully effective. In particular it appears as if the removal of PKCS#1 padding may leak timing information, which in turn could be used to recover session key bits. In Go 1.20, the crypto/tls library switched to a fully constant time RSA implementation, which we do not believe exhibits any timing side channels.	7.5	More Details
CVE-2023-40211	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in PickPlugins Post Grid Combo – 36+ Gutenberg Blocks.This issue affects Post Grid Combo – 36+ Gutenberg Blocks: from n/a through 2.2.50.	7.5	More Details
CVE-2023-48950	An issue in the box_col_len function in openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) after running a SELECT statement.	7.5	More Details
CVE-2023-31176	An Insufficient Entropy vulnerability in the Schweitzer Engineering Laboratories SEL-451 could allow an unauthenticated remote attacker to brute-force session tokens and bypass authentication. See product Instruction Manual Appendix A dated 20230830 for more details.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33097	Transient DOS in WLAN Firmware while processing a FTMR frame.	7.5	More Details
CVE-2023-48949	An issue in the box_add function in openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) after running a SELECT statement.	7.5	More Details
CVE-2023-39248	Dell OS10 Networking Switches running 10.5.2.x and above contain an Uncontrolled Resource Consumption (Denial of Service) vulnerability, when switches are configured with VLT and VRRP. A remote unauthenticated user can cause the network to be flooded leading to Denial of Service for actual network users. This is a high severity vulnerability as it allows an attacker to cause an outage of network. Dell recommends customers to upgrade at the earliest opportunity.	7.5	More Details
CVE-2023-43472	An issue in MLFlow versions 2.8.1 and before allows a remote attacker to obtain sensitive information via a crafted request to REST API.	7.5	More Details
CVE-2023-48964	Tenda i6 V1.0.0.8(3856) is vulnerable to Buffer Overflow via /goform/WifiMacFilterSet.	7.5	More Details
CVE-2023-48945	A stack overflow in openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-48948	An issue in the box_div function in openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) after running a SELECT statement.	7.5	More Details
CVE-2023-48963	Tenda i6 V1.0.0.8(3856) is vulnerable to Buffer Overflow via /goform/wifiSSIDget.	7.5	More Details
CVE-2023-48947	An issue in the cha_cmp function of openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) after running a SELECT statement.	7.5	More Details
CVE-2023-48946	An issue in the box_mpy function of openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) after running a SELECT statement.	7.5	More Details
CVE-2023-42580	Improper URL validation from MCSLaunch deeplink in Galaxy Store prior to version 4.5.64.4 allows attackers to execute JavaScript API to install APK from Galaxy Store.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42581	Improper URL validation from InstantPlay deeplink in Galaxy Store prior to version 4.5.64.4 allows attackers to execute JavaScript API to access data.	7.5	More Details
CVE-2023-40626	The language file parsing process could be manipulated to expose environment variables. Environment variables might contain sensible information.	7.5	More Details
CVE-2023-33098	Transient DOS while parsing WPA IES, when it is passed with length more than expected size.	7.5	More Details
CVE-2023-37572	Softing OPC Suite version 5.25 and before has Incorrect Access Control, allows attackers to obtain sensitive information via weak permissions in OSF_discovery service. The service executable could be changed or the service could be deleted.	7.5	More Details
CVE-2023-48951	An issue in the box_equal function in openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) after running a SELECT statement.	7.5	More Details
CVE-2023-42560	Heap out-of-bounds write vulnerability in dec_mono_audb of libsavsac.so prior to SMR Dec-2023 Release 1 allows an attacker to execute arbitrary code.	7.4	More Details
CVE-2020-36768	A vulnerability was found in rl-institut NESP2 Initial Release/1.0. It has been classified as critical. Affected is an unknown function of the file app/database.py. The manipulation 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 patch is identified as 07c0cdf36cf6a4345086d07b54423723a496af5e. It is recommended to apply a patch to fix this issue. VDB-246642 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2023-42568	Improper access control vulnerability in SmartManagerCN prior to SMR Dec-2023 Release 1 allows local attackers to access arbitrary files with system privilege.	7.3	More Details
CVE-2023-42567	Improper size check vulnerability in softsimd prior to SMR Dec-2023 Release 1 allows stack-based buffer overflow.	7.3	More Details
CVE-2023-42566	Out-of-bound write vulnerability in libsavsvc prior to SMR Dec-2023 Release 1 allows local attackers to execute arbitrary code.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42565	Improper input validation vulnerability in Smart Clip prior to SMR Dec-2023 Release 1 allows local attackers with shell privilege to execute arbitrary code.	7.3	More Details
CVE-2023-39257	Dell Rugged Control Center, version prior to 4.7, contains an Improper Access Control vulnerability. A local malicious standard user could potentially exploit this vulnerability to modify the content in an unsecured folder when product installation repair is performed, leading to privilege escalation on the system.	7.3	More Details
CVE-2023-39256	Dell Rugged Control Center, version prior to 4.7, contains an improper access control vulnerability. A local malicious standard user could potentially exploit this vulnerability to modify the content in an unsecured folder during product installation and upgrade, leading to privilege escalation on the system.	7.3	More Details
CVE-2023-48695	Azure RTOS USBX is a USB host, device, and on-the-go (OTG) embedded stack, that is fully integrated with Azure RTOS ThreadX. An attacker can cause remote code execution due to out of bounds write vulnerabilities in Azure RTOS USBX. The affected components include functions/processes in host and device classes, related to CDC ECM and RNDIS in RTOS v6.2.1 and below. The fixes have been included in USBX release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.3	More Details
CVE-2023-6218	In Progress MOVEit Transfer versions released before 2022.0.9 (14.0.9), 2022.1.10 (14.1.10), 2023.0.7 (15.0.7), a privilege escalation path associated with group administrators has been identified. It is possible for a group administrator to elevate a group members permissions to the role of an organization administrator.	7.2	More Details
CVE-2023-5108	The Easy Newsletter Signups WordPress plugin through 1.0.4 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin	7.2	More Details
CVE-2023-38003	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow a user with DATAACCESS privileges to execute routines that they should not have access to. IBM X-Force ID: 260214.	7.2	More Details
CVE-2023-44291	Dell DM5500 5.14.0.0 contains an OS command injection vulnerability in the appliance. A remote attacker with high privileges could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the underlying OS, with the privileges of the vulnerable application. Exploitation may lead to a system take over by an attacker.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49081	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Improper validation made it possible for an attacker to modify the HTTP request (e.g. to insert a new header) or create a new HTTP request if the attacker controls the HTTP version. The vulnerability only occurs if the attacker can control the HTTP version of the request. This issue has been patched in version 3.9.0.	7.2	More Details
CVE-2023-49701	Memory Corruption in SIM management while USIMPhase2init	7.2	More Details
CVE-2023-46956	SQL injection vulnerability in Packers and Movers Management System v.1.0 allows a remote attacker to execute arbitrary code via crafted payload to the /mpms/admin/?page=user/manage_user&id file.	7.2	More Details
CVE-2023-44221	Improper neutralization of special elements in the SMA100 SSL-VPN management interface allows a remote authenticated attacker with administrative privilege to inject arbitrary commands as a 'nobody' user, potentially leading to OS Command Injection Vulnerability.	7.2	More Details
CVE-2023-46086	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SERVIT Software Solutions affiliate-toolkit – WordPress Affiliate Plugin allows Reflected XSS.This issue affects affiliate-toolkit – WordPress Affiliate Plugin: from n/a through 3.4.3.	7.1	More Details
CVE-2023-48322	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eDoc Intelligence eDoc Employee Job Application – Best WordPress Job Manager for Employees allows Reflected XSS.This issue affects eDoc Employee Job Application – Best WordPress Job Manager for Employees: from n/a through 1.13.	7.1	More Details
CVE-2023-36682	Cross-Site Request Forgery (CSRF) vulnerability in Brainstorm Force US LLC Schema Pro allows Cross Site Request Forgery.This issue affects Schema Pro: from n/a through 2.7.7.	7.1	More Details
CVE-2023-48326	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pixelite Events Manager allows Reflected XSS.This issue affects Events Manager: from n/a through 6.4.5.	7.1	More Details
CVE-2023-40460	The ACEManager component of ALEOS 4.16 and earlier does not validate uploaded file names and types, which could potentially allow an authenticated user to perform client-side script execution within ACEManager, altering the device functionality until the device is restarted.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33333	Cross-Site Request Forgery (CSRF) vulnerability in Really Simple Plugins Complianz, Really Simple Plugins Complianz Premium allows Cross-Site Scripting (XSS).This issue affects Complianz: from n/a through 6.4.4; Complianz Premium: from n/a through 6.4.6.1.	7.1	More Details
CVE-2023-48314	Collabora Online is a collaborative online office suite based on LibreOffice technology. Users of Nextcloud with Collabora Online Built-in CODE Server app can be vulnerable to attack via proxy.php. This vulnerability has been fixed in Collabora Online - Built-in CODE Server (richdocumentscode) release 23.5.403. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.1	More Details
CVE-2023-38474	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Campaign Monitor Campaign Monitor for WordPress allows Reflected XSS.This issue affects Campaign Monitor for WordPress: from n/a through 2.8.12.	7.1	More Details
CVE-2023-47876	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Perfmatters allows Reflected XSS.This issue affects Perfmatters: from n/a through 2.1.6.	7.1	More Details
CVE-2023-48748	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Theme nectar Salient Core allows Reflected XSS.This issue affects Salient Core: from n/a through 2.0.2.	7.1	More Details
CVE-2023-47844	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Lim Kai Yang Grab & Save allows Reflected XSS.This issue affects Grab & Save: from n/a through 1.0.4.	7.1	More Details
CVE-2023-6217	In Progress MOVEit Transfer versions released before 2022.0.9 (14.0.9), 2022.1.10 (14.1.10), 2023.0.7 (15.0.7), a reflected cross-site scripting (XSS) vulnerability has been identified when MOVEit Gateway is used in conjunction with MOVEit Transfer. An attacker could craft a malicious payload targeting the system which comprises a MOVEit Gateway and MOVEit Transfer deployment. If a MOVEit user interacts with the crafted payload, the attacker would be able to execute malicious JavaScript within the context of the victim’s browser.	7.1	More Details
CVE-2023-47521	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Max Bond, AndreSC Q2W3 Post Order allows Reflected XSS.This issue affects Q2W3 Post Order: from n/a through 1.2.8.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38400	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kriesi Enfold - Responsive Multi-Purpose Theme allows Reflected XSS.This issue affects Enfold - Responsive Multi-Purpose Theme: from n/a through 5.6.4.	7.1	More Details
CVE-2023-44297	Dell PowerEdge platforms 16G Intel E5 BIOS and Dell Precision BIOS, version 1.4.4, contain active debug code security vulnerability. An unauthenticated physical attacker could potentially exploit this vulnerability, leading to information disclosure, information tampering, code execution, denial of service.	7.1	More Details
CVE-2023-33070	Transient DOS in Automotive OS due to improper authentication to the secure IO calls.	7.1	More Details
CVE-2023-48272	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in yonifre Maspik – Spam Blacklist allows Stored XSS.This issue affects Maspik – Spam Blacklist: from n/a through 0.9.2.	7.1	More Details
CVE-2023-48278	Cross-Site Request Forgery (CSRF) vulnerability in Nitin Rathod WP Forms Puzzle Captcha allows Stored XSS.This issue affects WP Forms Puzzle Captcha: from n/a through 4.1.	7.1	More Details
CVE-2023-6481	A serialization vulnerability in logback receiver component part of logback version 1.4.13, 1.3.13 and 1.2.12 allows an attacker to mount a Denial-Of-Service attack by sending poisoned data.	7.1	More Details
CVE-2023-48746	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PeepSo Community by PeepSo – Social Network, Membership, Registration, User Profiles allows Reflected XSS.This issue affects Community by PeepSo – Social Network, Membership, Registration, User Profiles: from n/a through 6.2.6.0.	7.1	More Details
CVE-2023-47870	Cross-Site Request Forgery (CSRF), Missing Authorization vulnerability in gVectors Team wpForo Forum wpforo allows Cross Site Request Forgery, Accessing Functionality Not Properly Constrained by ACLs leading to forced all users log out.This issue affects wpForo Forum: from n/a through 2.2.6.	7.1	More Details
CVE-2023-48752	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Happyforms Form builder to get in touch with visitors, grow your email list and collect payments — Happyforms allows Reflected XSS.This issue affects Form builder to get in touch with visitors, grow your email list and collect payments — Happyforms: from n/a through 1.25.9.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6378	A serialization vulnerability in logback receiver component part of logback version 1.4.11 allows an attacker to mount a Denial-Of-Service attack by sending poisoned data.	7.1	More Details
CVE-2023-42561	Heap out-of-bounds write vulnerability in bootloader prior to SMR Dec-2023 Release 1 allows a physical attacker to execute arbitrary code.	7.1	More Details
CVE-2023-47848	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tainacan.Org Tainacan allows Reflected XSS.This issue affects Tainacan: from n/a through 0.20.4.	7.1	More Details
CVE-2023-45084	An issue exists in SoftIron HyperCloud where drive caddy removal and reinsertion without a reboot may erroneously cause the system to recognize the caddy as new media and wipe all data on the drives due to a missing synchronization flaw, which impacts data availability and integrity. This issue only impacts SoftIron HyperCloud "density" storage nodes running HyperCloud software versions 1.0 to before 2.0.3.	7.0	More Details
CVE-2023-42577	Improper Access Control in Samsung Voice Recorder prior to versions 21.4.15.01 in Android 12 and Android 13, 21.4.50.17 in Android 14 allows physical attackers to access Voice Recorder information on the lock screen.	6.8	More Details
CVE-2023-49090	CarrierWave is a solution for file uploads for Rails, Sinatra and other Ruby web frameworks. CarrierWave has a Content-Type allowlist bypass vulnerability, possibly leading to XSS. The validation in `allowlisted_content_type?` determines Content-Type permissions by performing a partial match. If the `content_type` argument of `allowlisted_content_type?` is passed a value crafted by the attacker, Content-Types not included in the `content_type_allowlist` will be allowed. This issue has been patched in versions 2.2.5 and 3.0.5.	6.8	More Details
CVE-2023-48698	Azure RTOS USBX is a USB host, device, and on-the-go (OTG) embedded stack, that is fully integrated with Azure RTOS ThreadX. An attacker can cause remote code execution due to expired pointer dereference vulnerabilities in Azure RTOS USBX. The affected components include functions/processes in host stack and host classes, related to device linked classes, GSER and HID in RTOS v6.2.1 and below. The fixes have been included in USBX release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.8	More Details
CVE-2023-24047	An Insecure Credential Management issue discovered in Connectize AC21000 G6 641.139.1.1256 allows attackers to gain escalated privileges via use of weak hashing algorithm.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48694	Azure RTOS USBX is a USB host, device, and on-the-go (OTG) embedded stack, that is fully integrated with Azure RTOS ThreadX. An attacker can cause remote code execution due to expired pointer dereference and type confusion vulnerabilities in Azure RTOS USBX. The affected components include functions/processes in host stack and host class, related to device linked classes, ASIX, Prolific, SWAR, audio, CDC ECM in RTOS v6.2.1 and below. The fixes have been included in USBX release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.8	More Details
CVE-2023-49087	xml-security is a library that implements XML signatures and encryption. Validation of an XML signature requires verification that the hash value of the related XML-document matches a specific DigestValue-value, but also that the cryptographic signature on the SignedInfo-tree (the one that contains the DigestValue) verifies and matches a trusted public key. If an attacker somehow (i.e. by exploiting a bug in PHP's canonicalization function) manages to manipulate the canonicalized version's DigestValue, it would be possible to forge the signature. This issue has been patched in version 1.6.12 and 5.0.0-alpha.13.	6.8	More Details
CVE-2023-24046	An issue was discovered on Connectize AC21000 G6 641.139.1.1256 allows attackers to run arbitrary commands via use of a crafted string in the ping utility.	6.8	More Details
CVE-2023-49700	Security best practices violations, a string operation in Streamingmedia will write past the end of fixed-size destination buffer if the source buffer is too large.	6.7	More Details
CVE-2023-32848	In vdec, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08163896; Issue ID: ALPS08163896.	6.7	More Details
CVE-2023-32863	In display drm, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07326314; Issue ID: ALPS07326314.	6.7	More Details
CVE-2023-42563	Integer overflow vulnerability in landmarkCopyImageToNative of libFacePreProcessingjni.camera.samsung.so prior to SMR Dec-2023 Release 1 allows attacker to trigger heap overflow.	6.7	More Details
CVE-2023-42562	Integer overflow vulnerability in detectionFindFaceSupportMultiInstance of libFacePreProcessingjni.camera.samsung.so prior to SMR Dec-2023 Release 1 allows attacker to trigger heap overflow.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42722	In camera service, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed	6.7	More Details
CVE-2023-49699	Memory Corruption in IMS while calling VoLTE Streamingmedia Interface	6.7	More Details
CVE-2023-32864	In display drm, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292187; Issue ID: ALPS07292187.	6.7	More Details
CVE-2023-32849	In cmdq, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08161758; Issue ID: ALPS08161758.	6.7	More Details
CVE-2023-32855	In aee, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07909204; Issue ID: ALPS07909204.	6.7	More Details
CVE-2023-32862	In display, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388762; Issue ID: ALPS07388762.	6.7	More Details
CVE-2023-32861	In display, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08059081; Issue ID: ALPS08059081.	6.7	More Details
CVE-2023-32860	In display, there is a possible classic buffer overflow due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929788; Issue ID: ALPS07929788.	6.7	More Details
CVE-2023-32859	In meta, there is a possible classic buffer overflow due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08000473; Issue ID: ALPS08000473.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32865	In display drm, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363456; Issue ID: ALPS07363456.	6.7	More Details
CVE-2023-33024	Memory corruption while sending SMS from AP firmware.	6.7	More Details
CVE-2023-32866	In mmp, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07342152; Issue ID: ALPS07342152.	6.7	More Details
CVE-2023-28580	Memory corruption in WLAN Host while setting the PMK length in PMK length in internal cache.	6.7	More Details
CVE-2023-32867	In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560793; Issue ID: ALPS07560793.	6.7	More Details
CVE-2023-22668	Memory Corruption in Audio while invoking IOCTLs calls from the user-space.	6.7	More Details
CVE-2023-28579	Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length.	6.7	More Details
CVE-2023-22383	Memory Corruption in camera while installing a fd for a particular DMA buffer.	6.7	More Details
CVE-2023-32854	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08240132; Issue ID: ALPS08240132.	6.7	More Details
CVE-2023-32870	In display drm, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363740; Issue ID: ALPS07363740.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48696	Azure RTOS USBX is a USB host, device, and on-the-go (OTG) embedded stack, that is fully integrated with Azure RTOS ThreadX. An attacker can cause remote code execution due to expired pointer dereference vulnerabilities in Azure RTOS USBX. The affected components include components in host class, related to CDC ACM in RTOS v6.2.1 and below. The fixes have been included in USBX release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.7	More Details
CVE-2023-32869	In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363632; Issue ID: ALPS07363689.	6.7	More Details
CVE-2023-32853	In rpmb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648764; Issue ID: ALPS07648764.	6.7	More Details
CVE-2023-21634	Memory Corruption in Radio Interface Layer while sending an SMS or writing an SMS to SIM.	6.7	More Details
CVE-2023-32868	In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363632; Issue ID: ALPS07363632.	6.7	More Details
CVE-2023-6449	The Contact Form 7 plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the 'validate' function and insufficient blocklisting on the 'wpcf7_antiscript_file_name' function in versions up to, and including, 5.8.3. This makes it possible for authenticated attackers with editor-level capabilities or above to upload arbitrary files on the affected site's server, but due to the htaccess configuration, remote code cannot be executed in most cases. By default, the file will be deleted from the server immediately. However, in some cases, other plugins may make it possible for the file to live on the server longer. This can make remote code execution possible when combined with another vulnerability, such as local file inclusion.	6.6	More Details
CVE-2023-42564	Improper access control in knoxcustom service prior to SMR Dec-2023 Release 1 allows attacker to send broadcast with system privilege.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47854	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Howard Ehrenberg Parallax Image allows Stored XSS.This issue affects Parallax Image: from n/a through 1.7.1.	6.5	More Details
CVE-2023-32291	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MonsterInsights Pro allows Stored XSS.This issue affects MonsterInsights Pro: from n/a through 8.14.1.	6.5	More Details
CVE-2023-40090	In BTM_BleVerifySignature of btm_ble.cc, there is a possible way to bypass signature validation due to side channel information disclosure. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	6.5	More Details
CVE-2023-49653	Jenkins Jira Plugin 3.11 and earlier does not set the appropriate context for credentials lookup, allowing attackers with Item/Configure permission to access and capture credentials they are not entitled to.	6.5	More Details
CVE-2023-48289	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SpreadsheetConverter Import Spreadsheets from Microsoft Excel allows Stored XSS.This issue affects Import Spreadsheets from Microsoft Excel: from n/a through 10.1.3.	6.5	More Details
CVE-2023-47851	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Akhtarujjaman Shuvo Bootstrap Shortcodes Ultimate allows Stored XSS.This issue affects Bootstrap Shortcodes Ultimate: from n/a through 4.3.1.	6.5	More Details
CVE-2023-5990	The Interactive Contact Form and Multi Step Form Builder with Drag & Drop Editor WordPress plugin before 3.4.2 does not have CSRF checks on some of its form actions such as deletion and duplication, which could allow attackers to make logged in admin perform such actions via CSRF attacks	6.5	More Details
CVE-2023-47850	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PeepSo Community by PeepSo – Social Network, Membership, Registration, User Profiles allows Stored XSS.This issue affects Community by PeepSo – Social Network, Membership, Registration, User Profiles: from n/a through 6.2.2.0.	6.5	More Details
CVE-2023-47777	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Automattic WooCommerce, Automattic WooCommerce Blocks allows Stored XSS.This issue affects WooCommerce: from n/a through 8.1.1; WooCommerce Blocks: from n/a through 11.1.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47505	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Elementor.Com Elementor allows Cross-Site Scripting (XSS).This issue affects Elementor: from n/a through 3.16.4.	6.5	More Details
CVE-2023-45050	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Automattic Jetpack – WP Security, Backup, Speed, & Growth allows Stored XSS.This issue affects Jetpack – WP Security, Backup, Speed, & Growth: from n/a through 12.8-a.1.	6.5	More Details
CVE-2023-48336	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cybernetikz Easy Social Icons allows Stored XSS.This issue affects Easy Social Icons: from n/a through 3.2.4.	6.5	More Details
CVE-2023-5884	The Word Balloon WordPress plugin before 4.20.3 does not protect some of its actions against CSRF attacks, allowing an unauthenticated attacker to trick a logged in user to delete arbitrary avatars by clicking a link.	6.5	More Details
CVE-2023-44306	Dell DM5500 contains a path traversal vulnerability in the appliance. A remote attacker with high privileges could potentially exploit this vulnerability to overwrite configuration files stored on the server filesystem.	6.5	More Details
CVE-2023-40674	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Lasso Simple URLs – Link Cloaking, Product Displays, and Affiliate Link Management allows Stored XSS.This issue affects Simple URLs – Link Cloaking, Product Displays, and Affiliate Link Management: from n/a through 118.	6.5	More Details
CVE-2023-5979	The eCommerce Product Catalog Plugin for WordPress plugin before 3.3.26 does not have CSRF checks in some of its admin pages, which could allow attackers to make logged-in users perform unwanted actions via CSRF attacks, such as delete all products	6.5	More Details
CVE-2023-47701	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 266166.	6.5	More Details
CVE-2023-49620	Before DolphinScheduler version 3.1.0, the login user could delete UDF function in the resource center unauthorized (which almost used in sql task), with unauthorized access vulnerability (IDOR), but after version 3.1.0 we fixed this issue. We mark this cve as moderate level because it still requires user login to operate, please upgrade to version 3.1.0 to avoid this vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48894	Incorrect Access Control vulnerability in jshERP V3.3 allows attackers to obtain sensitive information via the doFilter function.	6.5	More Details
CVE-2023-26533	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Gesundheit Bewegt GmbH Zippy.This issue affects Zippy: from n/a through 1.6.1.	6.5	More Details
CVE-2023-47853	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in myCred myCred – Points, Rewards, Gamification, Ranks, Badges & Loyalty Plugin allows Stored XSS.This issue affects myCred – Points, Rewards, Gamification, Ranks, Badges & Loyalty Plugin: from n/a through 2.6.1.	6.5	More Details
CVE-2023-26941	Weak encryption mechanisms in RFID Tags in Yale Conexis L1 v1.1.0 allows attackers to create a cloned tag via physical proximity to the original.	6.5	More Details
CVE-2023-26942	Weak encryption mechanisms in RFID Tags in Yale IA-210 Alarm v1.0 allows attackers to create a cloned tag via physical proximity to the original.	6.5	More Details
CVE-2023-26943	Weak encryption mechanisms in RFID Tags in Yale Keyless Lock v1.0 allows attackers to create a cloned tag via physical proximity to the original.	6.5	More Details
CVE-2023-45178	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5 CLI is vulnerable to a denial of service when a specially crafted request is used. IBM X-Force ID: 268073.	6.5	More Details
CVE-2023-37868	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Leap13 Premium Addons PRO.This issue affects Premium Addons PRO: from n/a through 2.9.0.	6.5	More Details
CVE-2023-49914	InteraXon Muse 2 devices allow remote attackers to cause a denial of service (incorrect Muse App report of an outstanding, calm meditation state) via a 480 MHz RF carrier that is modulated by a "false" brain wave, aka a Brain-Hack attack. For example, the Muse App does not display the reception of a strong RF carrier, and alert the user that a report may be misleading if this carrier has been modulated by a low-frequency signal.	6.5	More Details
CVE-2023-44143	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bamboo Mcr Bamboo Columns allows Stored XSS.This issue affects Bamboo Columns: from n/a through 1.6.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45609	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in POWR.Io Contact Form – Custom Builder, Payment Form, and More allows Stored XSS.This issue affects Contact Form – Custom Builder, Payment Form, and More: from n/a through 2.1.0.	6.5	More Details
CVE-2023-42579	Improper usage of insecure protocol (i.e. HTTP) in SogouSDK of Chinese Samsung Keyboard prior to versions 5.3.70.1 in Android 11, 5.4.60.49, 5.4.85.5, 5.5.00.58 in Android 12, and 5.6.00.52, 5.6.10.42, 5.7.00.45 in Android 13 allows adjacent attackers to access keystroke data using Man-in-the-Middle attack.	6.5	More Details
CVE-2023-42578	Improper handling of insufficient permissions or privileges vulnerability in Samsung Data Store prior to version 5.2.00.7 allows remote attackers to access location information without permission.	6.5	More Details
CVE-2023-34388	An Improper Authentication vulnerability in the Schweitzer Engineering Laboratories SEL-451 could allow a remote unauthenticated attacker to potentially perform session hijacking attack and bypass authentication. See product Instruction Manual Appendix A dated 20230830 for more details.	6.5	More Details
CVE-2023-4518	A vulnerability exists in the input validation of the GOOSE messages where out of range values received and processed by the IED caused a reboot of the device. In order for an attacker to exploit the vulnerability, goose receiving blocks need to be configured.	6.5	More Details
CVE-2023-26024	IBM Planning Analytics on Cloud Pak for Data 4.0 could allow an attacker on a shared network to obtain sensitive information caused by insecure network communication. IBM X-Force ID: 247898.	6.5	More Details
CVE-2023-47872	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gVectors Team wpForo Forum allows Stored XSS.This issue affects wpForo Forum: from n/a through 2.2.3.	6.5	More Details
CVE-2023-47827	Incorrect Authorization vulnerability in NicheAddons Events Addon for Elementor allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Events Addon for Elementor: from n/a through 2.1.3.	6.5	More Details
CVE-2023-42916	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 17.1.2 and iPadOS 17.1.2, macOS Sonoma 14.1.2, Safari 17.1.2. Processing web content may disclose sensitive information. Apple is aware of a report that this issue may have been exploited against versions of iOS before iOS 16.7.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5105	The Frontend File Manager Plugin WordPress plugin before 22.6 has a vulnerability that allows an Editor+ user to bypass the file download logic and download files such as `wp-config.php`	6.5	More Details
CVE-2023-48749	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Theme nectar Salient Core allows Stored XSS.This issue affects Salient Core: from n/a through 2.0.2.	6.5	More Details
CVE-2023-48321	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ahmed Kaludi, Mohammed Kaludi AMP for WP – Accelerated Mobile Pages allows Stored XSS.This issue affects AMP for WP – Accelerated Mobile Pages: from n/a through 1.0.88.1.	6.5	More Details
CVE-2023-47877	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Perfmatters allows Stored XSS.This issue affects Perfmatters: from n/a before 2.2.0.	6.5	More Details
CVE-2023-34030	Cross-Site Request Forgery (CSRF) vulnerability in Really Simple Plugins Complianz, Really Simple Plugins Complianz Premium allows Cross-Site Request Forgery.This issue affects Complianz: from n/a through 6.4.5; Complianz Premium: from n/a through 6.4.7.	6.5	More Details
CVE-2023-4770	An uncontrolled search path element vulnerability has been found on 4D and 4D server Windows executables applications, affecting version 19 R8 100218. This vulnerability consists in a DLL hijacking by replacing x64 shfolder.dll in the installation path, causing an arbitrary code execution.	6.5	More Details
CVE-2023-48317	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vikas Vatsa Display Custom Post allows Stored XSS.This issue affects Display Custom Post: from n/a through 2.2.1.	6.5	More Details
CVE-2023-6419	A vulnerability has been reported in Voovi Social Networking Script version 1.0 that allows a XSS via editprofile.php in multiple parameters, the exploitation of which could allow a remote attacker to send a specially crafted JavaScript payload and partially take over the browser session of an authenticated user.	6.5	More Details
CVE-2023-6420	A vulnerability has been reported in Voovi Social Networking Script version 1.0 that allows a XSS via signup2.php in the emailadd parameter, the exploitation of which could allow a remote attacker to send a specially crafted JavaScript payload and partially take over the browser session of an authenticated user.	6.5	More Details
CVE-2023-48333	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Pluggabl LLC Booster for WooCommerce.This issue affects Booster for WooCommerce: from n/a through 7.1.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48697	Azure RTOS USBX is a USB host, device, and on-the-go (OTG) embedded stack, that is fully integrated with Azure RTOS ThreadX. An attacker can cause remote code execution due to memory buffer and pointer vulnerabilities in Azure RTOS USBX. The affected components include functions/processes in pictbridge and host class, related to PIMA, storage, CDC ACM, ECM, audio, hub in RTOS v6.2.1 and below. The fixes have been included in USBX release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.4	More Details
CVE-2023-6464	A vulnerability was found in SourceCodester User Registration and Login System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /endpoint/add-user.php. The manipulation of the argument user leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-246614 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-49276	Uptime Kuma is an open source self-hosted monitoring tool. In affected versions the Google Analytics element in vulnerable to Attribute Injection leading to Cross-Site-Scripting (XSS). Since the custom status interface can set an independent Google Analytics ID and the template has not been sanitized, there is an attribute injection vulnerability here, which can lead to XSS attacks. This vulnerability has been addressed in commit \`f28dccf4e\` which is included in release version 1.23.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.3	More Details
CVE-2023-44295	Dell PowerScale OneFS versions 8.2.2.x through 9.6.0.x contains an improper control of a resource through its lifetime vulnerability. A low privilege attacker could potentially exploit this vulnerability, leading to loss of information, and information disclosure.	6.3	More Details
CVE-2023-6402	A vulnerability, which was classified as critical, was found in PHPGurukul Nipah Virus Testing Management System 1.0. This affects an unknown part of the file add-phlebotomist.php. The manipulation of the argument empid 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-246423.	6.3	More Details
CVE-2023-49289	Ajax.NET Professional (AjaxPro) is an AJAX framework for Microsoft ASP.NET which will create proxy JavaScript classes that are used on client-side to invoke methods on the web server. Affected versions of this package are vulnerable cross site scripting attacks. Releases before version 21.12.22.1 are affected. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6435	A vulnerability has been discovered in BigProf Online Invoicing System 2.6, which does not sufficiently encode user-controlled input, resulting in persistent XSS through /inventory/batches_view.php, in the FirstRecord parameter. Exploitation of this vulnerability could allow an attacking user to store dangerous JavaScript payloads on the system that will be triggered when the page loads.	6.3	More Details
CVE-2023-6424	A vulnerability has been discovered in BigProf Online Clinic Management System 2.2, which does not sufficiently encode user-controlled input, resulting in persistent XSS through /clinic/disease_symptoms_view.php, in the FirstRecord parameter. Exploitation of this vulnerability could allow an attacking user to store dangerous JavaScript payloads on the system that will be triggered when the page loads.	6.3	More Details
CVE-2023-6434	A vulnerability has been discovered in BigProf Online Invoicing System 2.6, which does not sufficiently encode user-controlled input, resulting in persistent XSS through /inventory/sections_view.php, in the FirstRecord parameter. Exploitation of this vulnerability could allow an attacking user to store dangerous JavaScript payloads on the system that will be triggered when the page loads.	6.3	More Details
CVE-2023-6430	A vulnerability has been discovered in BigProf Online Invoicing System 2.6, which does not sufficiently encode user-controlled input, resulting in persistent XSS through /inventory/transactions_view.php, in the FirstRecord parameter. Exploitation of this vulnerability could allow an attacking user to store dangerous JavaScript payloads on the system that will be triggered when the page loads.	6.3	More Details
CVE-2023-6425	A vulnerability has been discovered in BigProf Online Clinic Management System 2.2, which does not sufficiently encode user-controlled input, resulting in persistent XSS through /clinic/medical_records_view.php, in the FirstRecord parameter. Exploitation of this vulnerability could allow an attacking user to store dangerous JavaScript payloads on the system that will be triggered when the page loads.	6.3	More Details
CVE-2023-6422	A vulnerability has been discovered in BigProf Online Clinic Management System 2.2, which does not sufficiently encode user-controlled input, resulting in persistent XSS through /clinic/patients_view.php, in the FirstRecord parameter. Exploitation of this vulnerability could allow an attacking user to store dangerous JavaScript payloads on the system that will be triggered when the page loads.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6426	A vulnerability has been discovered in BigProf Online Invoicing System 2.6, which does not sufficiently encode user-controlled input, resulting in persistent XSS through /invoicing/app/invoices_view.php, in the FirstRecord parameter. Exploitation of this vulnerability could allow an attacking user to store dangerous JavaScript payloads on the system that will be triggered when the page loads.	6.3	More Details
CVE-2023-6427	A vulnerability has been discovered in BigProf Online Invoicing System 2.6, which does not sufficiently encode user-controlled input, resulting in persistent XSS through /invoicing/app/invoices_view.php, in the FirstRecord parameter. Exploitation of this vulnerability could allow an attacking user to store dangerous JavaScript payloads on the system that will be triggered when the page loads.	6.3	More Details
CVE-2023-6428	A vulnerability has been discovered in BigProf Online Invoicing System 2.6, which does not sufficiently encode user-controlled input, resulting in persistent XSS through /invoicing/app/items_view.php, in the FirstRecord parameter. Exploitation of this vulnerability could allow an attacking user to store dangerous JavaScript payloads on the system that will be triggered when the page loads.	6.3	More Details
CVE-2023-6429	A vulnerability has been discovered in BigProf Online Invoicing System 2.6, which does not sufficiently encode user-controlled input, resulting in persistent XSS through /invoicing/app/clients_view.php, in the FirstRecord parameter. Exploitation of this vulnerability could allow an attacking user to store dangerous JavaScript payloads on the system that will be triggered when the page loads.	6.3	More Details
CVE-2023-6423	A vulnerability has been discovered in BigProf Online Clinic Management System 2.2, which does not sufficiently encode user-controlled input, resulting in persistent XSS through /clinic/events_view.php, in the FirstRecord parameter. Exploitation of this vulnerability could allow an attacking user to store dangerous JavaScript payloads on the system that will be triggered when the page loads.	6.3	More Details
CVE-2023-6431	A vulnerability has been discovered in BigProf Online Invoicing System 2.6, which does not sufficiently encode user-controlled input, resulting in persistent XSS through /inventory/categories_view.php, in the FirstRecord parameter. Exploitation of this vulnerability could allow an attacking user to store dangerous JavaScript payloads on the system that will be triggered when the page loads.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6432	A vulnerability has been discovered in BigProf Online Invoicing System 2.6, which does not sufficiently encode user-controlled input, resulting in persistent XSS through /inventory/items_view.php, in the FirstRecord parameter. Exploitation of this vulnerability could allow an attacking user to store dangerous JavaScript payloads on the system that will be triggered when the page loads.	6.3	More Details
CVE-2023-6433	A vulnerability has been discovered in BigProf Online Invoicing System 2.6, which does not sufficiently encode user-controlled input, resulting in persistent XSS through /inventory/suppliers_view.php, in the FirstRecord parameter. Exploitation of this vulnerability could allow an attacking user to store dangerous JavaScript payloads on the system that will be triggered when the page loads.	6.3	More Details
CVE-2023-5141	The BSK Contact Form 7 Blacklist WordPress plugin through 1.0.1 does not sanitise and escape the inserted_count parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-5951	The Welcart e-Commerce WordPress plugin before 2.9.5 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-6461	Cross-site Scripting (XSS) - Reflected in GitHub repository viliusle/minipaint prior to 4.14.0.	6.1	More Details
CVE-2023-49926	app/Lib/Tools/EventTimelineTool.php in MISP before 2.4.179 allows XSS in the event timeline widget.	6.1	More Details
CVE-2023-49293	Vite is a website frontend framework. When Vite's HTML transformation is invoked manually via `server.transformIndexHtml`, the original request URL is passed in unmodified, and the `html` being transformed contains inline module scripts (`<script type="module">...</script>`), it is possible to inject arbitrary HTML into the transformed output by supplying a malicious URL query string to `server.transformIndexHtml`. Only apps using `appType: 'custom'` and using the default Vite HTML middleware are affected. The HTML entry must also contain an inline script. The attack requires a user to click on a malicious URL while running the dev server. Restricted files aren't exposed to the attacker. This issue has been addressed in vite@5.0.5, vite@4.5.1, and vite@4.4.12. There are no known workarounds for this vulnerability.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5210	The AMP+ Plus WordPress plugin through 3.0 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-48815	kkFileView v4.3.0 is vulnerable to Incorrect Access Control.	6.1	More Details
CVE-2023-6027	A critical flaw has been identified in elijaa/phpmemcachedadmin affecting version 1.3.0, specifically related to a stored XSS vulnerability. This vulnerability allows malicious actors to insert a carefully crafted JavaScript payload. The issue arises from improper encoding of user-controlled entries in the "/pmcadmin/configure.php" parameter.	6.1	More Details
CVE-2023-44402	Electron is an open source framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. This only impacts apps that have the \`embeddedAsarIntegrityValidation\` and \`onlyLoadAppFromAsar\` fuses enabled. Apps without these fuses enabled are not impacted. This issue is specific to macOS as these fuses are only currently supported on macOS. Specifically this issue can only be exploited if your app is launched from a filesystem the attacker has write access too. i.e. the ability to edit files inside the \`.app\` bundle on macOS which these fuses are supposed to protect against. There are no app side workarounds, you must update to a patched version of Electron.	6.1	More Details
CVE-2023-46674	An issue was identified that allowed the unsafe deserialization of java objects from hadoop or spark configuration properties that could have been modified by authenticated users. Elastic would like to thank Yakov Shafranovich, with Amazon Web Services for reporting this issue.	6.0	More Details
CVE-2023-5767	A vulnerability exists in the webserver that affects the RTU500 series product versions listed below. A malicious actor could perform cross-site scripting on the webserver due to an RDT language file being improperly sanitized.	6.0	More Details
CVE-2023-28586	Information disclosure when the trusted application metadata symbol addresses are accessed while loading an ELF in TEE.	6.0	More Details
CVE-2023-42558	Out of bounds write vulnerability in HDCP in HAL prior to SMR Dec-2023 Release 1 allows attacker to perform code execution.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48329	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodeBard Fast Custom Social Share by CodeBard allows Stored XSS.This issue affects Fast Custom Social Share by CodeBard: from n/a through 1.1.1.	5.9	More Details
CVE-2023-48320	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebDorado SpiderVPlayer allows Stored XSS.This issue affects SpiderVPlayer: from n/a through 1.5.22.	5.9	More Details
CVE-2023-5332	Patch in third party library Consul requires 'enable-script-checks' to be set to False. This was required to enable a patch by the vendor. Without this setting the patch could be bypassed. This only affects GitLab-EE.	5.9	More Details
CVE-2023-5768	A vulnerability exists in the HCI IEC 60870-5-104 that affects the RTU500 series product versions listed below. Incomplete or wrong received APDU frame layout may cause blocking on link layer. Error reason was an endless blocking when reading incoming frames on link layer with wrong length information of APDU or delayed reception of data octets. Only communication link of affected HCI IEC 60870-5-104 is blocked. If attack sequence stops the communication to the previously attacked link gets normal again.	5.9	More Details
CVE-2023-41127	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Evergreen Content Poster Evergreen Content Poster – Auto Post and Schedule Your Best Content to Social Media allows Stored XSS.This issue affects Evergreen Content Poster – Auto Post and Schedule Your Best Content to Social Media: from n/a through 1.3.6.1.	5.9	More Details
CVE-2023-47124	Traefik is an open source HTTP reverse proxy and load balancer. When Traefik is configured to use the \`HTTPChallenge\` to generate and renew the Let's Encrypt TLS certificates, the delay authorized to solve the challenge (50 seconds) can be exploited by attackers to achieve a \`slowloris attack\`. This vulnerability has been patch in version 2.10.6 and 3.0.0-beta5. Users are advised to upgrade. Users unable to upgrade should replace the \`HTTPChallenge\` with the \`TLSChallenge\` or the \`DNSChallenge\`.	5.9	More Details
CVE-2023-41128	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Iqonic Design WP Roadmap – Product Feedback Board allows Stored XSS.This issue affects WP Roadmap – Product Feedback Board: from n/a through 1.0.8.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34018	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SoundCloud Inc. SoundCloud Shortcode allows Stored XSS.This issue affects SoundCloud Shortcode: from n/a through 3.1.0.	5.9	More Details
CVE-2023-42570	Improper access control vulnerability in KnoxCustomManagerService prior to SMR Dec-2023 Release 1 allows attacker to access device SIM PIN.	5.9	More Details
CVE-2023-41136	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Laurence/OhMyBox.Info Simple Long Form allows Stored XSS.This issue affects Simple Long Form: from n/a through 2.2.2.	5.9	More Details
CVE-2023-45066	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Smackcoders Export All Posts, Products, Orders, Refunds & Users.This issue affects Export All Posts, Products, Orders, Refunds & Users: from n/a through 2.4.1.	5.9	More Details
CVE-2023-46167	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 federated server is vulnerable to a denial of service when a specially crafted cursor is used. IBM X-Force ID: 269367.	5.9	More Details
CVE-2023-40680	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Team Yoast Yoast SEO allows Stored XSS.This issue affects Yoast SEO: from n/a through 21.0.	5.9	More Details
CVE-2023-40692	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, 11.5 is vulnerable to denial of service under extreme stress conditions. IBM X-Force ID: 264807.	5.9	More Details
CVE-2023-39921	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Molongui Author Box, Guest Author and Co-Authors for Your Posts – Molongui allows Stored XSS.This issue affects Author Box, Guest Author and Co-Authors for Your Posts – Molongui: from n/a through 4.6.19.	5.9	More Details
CVE-2023-49083	cryptography is a package designed to expose cryptographic primitives and recipes to Python developers. Calling `load_pem_pkcs7_certificates` or `load_der_pkcs7_certificates` could lead to a NULL-pointer dereference and segfault. Exploitation of this vulnerability poses a serious risk of Denial of Service (DoS) for any application attempting to deserialize a PKCS7 blob/certificate. The consequences extend to potential disruptions in system availability and stability. This vulnerability has been patched in version 41.0.6.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48737	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PT Trijaya Digital Grup TriPay Payment Gateway allows Stored XSS.This issue affects TriPay Payment Gateway: from n/a through 3.2.7.	5.9	More Details
CVE-2023-42019	IBM InfoSphere Information Server 11.7 could allow a remote attacker to cause a denial of service due to improper input validation. IBM X-Force ID: 265161.	5.9	More Details
CVE-2023-43628	An integer underflow vulnerability exists in the NTRIP Stream Parsing functionality of GPSd 3.25.1~dev. A specially crafted network packet can lead to memory corruption. An attacker can send a malicious packet to trigger this vulnerability.	5.9	More Details
CVE-2023-48743	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Paul Menard Simply Exclude allows Reflected XSS.This issue affects Simply Exclude: from n/a through 2.0.6.6.	5.8	More Details
CVE-2023-42557	Out-of-bound write vulnerability in libIfaaCa prior to SMR Dec-2023 Release 1 allows local system attackers to execute arbitrary code.	5.6	More Details
CVE-2023-40092	In verifyShortcutInfoPackage of ShortcutService.java, there is a possible way to see another user's image due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-40075	In forceReplaceShortcutInner of ShortcutPackage.java, there is a possible way to register unlimited packages due to a missing bounds check. This could lead to local denial of service which results in a boot loop with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-40074	In saveToXml of PersistableBundle.java, invalid data could lead to local persistent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-40083	In parse_gap_data of utils.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-40073	In visitUris of Notification.java, there is a possible cross-user media read due to Confused Deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40081	In loadMediaDataInBgForResumption of MediaDataManager.kt, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-40076	In createPendingIntent of CredentialManagerUi.java, there is a possible way to access credentials from other users due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-35668	In visitUris of Notification.java, there is a possible way to display images from another user due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-45781	In parse_gap_data of utils.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-40098	In mOnDone of NotificationConversationInfo.java, there is a possible way to access app notification data of another user due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-42699	In omacp service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42672	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42678	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42673	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42674	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42675	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42676	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42723	In camera service, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-42721	In flv extractor, there is a possible missing verification incorrect input. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-42720	In video service, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-42719	In video service, there is a possible out of bounds read due to a incorrect bounds check. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-42718	In dialer, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42715	In telephony service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42714	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42713	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42712	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42711	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42710	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42709	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42708	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42707	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42706	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42705	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42704	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42703	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42702	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42701	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42700	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42698	In omacp service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42697	In omacp service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42728	In phasecheckserver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-42677	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42730	In IMS service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42741	In telecom service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42671	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2022-48462	In wifi service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2022-48463	In wifi service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-42744	In telecom service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-42742	In sysui, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42749	In enginnermode service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42737	In telecom service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2022-48464	In wifi service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-42734	In telephony service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42733	In telephony service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42732	In telephony service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-44300	Dell DM5500 5.14.0.0, contain a Plain-text Password Storage Vulnerability in the appliance. A local attacker with privileges could potentially exploit this vulnerability, leading to the disclosure of certain service credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	5.5	More Details
CVE-2023-6137	Cross-Site Request Forgery (CSRF) vulnerability in finnj Frontier Post allows Cross Site Request Forgery.This issue affects Frontier Post: from n/a through 6.1.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49282	msgraph-sdk-php is the Microsoft Graph Library for PHP. The Microsoft Graph PHP SDK published packages which contained test code that enabled the use of the phpInfo() function from any application that could access and execute the file at vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php. The phpInfo function exposes system information. The vulnerability affects the GetPhpInfo.php script of the PHP SDK which contains a call to the phpinfo() function. This vulnerability requires a misconfiguration of the server to be present so it can be exploited. For example, making the PHP application's /vendor directory web accessible. The combination of the vulnerability and the server misconfiguration would allow an attacker to craft an HTTP request that executes the phpinfo() method. The attacker would then be able to get access to system information like configuration, modules, and environment variables and later on use the compromised secrets to access additional data. This problem has been patched in versions 1.109.1 and 2.0.0-RC5. If an immediate deployment with the updated vendor package is not available, you can perform the following temporary workarounds: delete the `vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php` file, remove access to the `/vendor` directory, or disable the phpinfo function.	5.4	More Details
CVE-2023-44383	October is a Content Management System (CMS) and web platform to assist with development workflow. A user with access to the media manager that stores SVG files could create a stored XSS attack against themselves and any other user with access to the media manager when SVG files are supported. This issue has been patched in version 3.5.2.	5.4	More Details
CVE-2023-48282	Cross-Site Request Forgery (CSRF) vulnerability in Andrea Landonio Taxonomy filter allows Cross Site Request Forgery.This issue affects Taxonomy filter: from n/a through 2.2.9.	5.4	More Details
CVE-2023-48330	Cross-Site Request Forgery (CSRF) vulnerability in Mike Strand Bulk Comment Remove allows Cross Site Request Forgery.This issue affects Bulk Comment Remove: from n/a through 2.	5.4	More Details
CVE-2023-48334	Cross-Site Request Forgery (CSRF) vulnerability in DAEXT League Table allows Cross Site Request Forgery.This issue affects League Table: from n/a through 1.13.	5.4	More Details
CVE-2023-48744	Cross-Site Request Forgery (CSRF) vulnerability in Offshore Web Master Availability Calendar allows Cross Site Request Forgery.This issue affects Availability Calendar: from n/a through 1.2.6.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42022	IBM InfoSphere Information Server 11.7 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: 265938.	5.4	More Details
CVE-2023-48754	Cross-Site Request Forgery (CSRF) vulnerability in Wap Nepal Delete Post Revisions In WordPress allows Cross Site Request Forgery.This issue affects Delete Post Revisions In WordPress: from n/a through 4.6.	5.4	More Details
CVE-2023-42576	Improper Authentication vulnerability in Samsung Pass prior to version 4.3.00.17 allows physical attackers to bypass authentication due to invalid exception handler.	5.4	More Details
CVE-2023-42575	Improper Authentication vulnerability in Samsung Pass prior to version 4.3.00.17 allows physical attackers to bypass authentication due to invalid flag setting.	5.4	More Details
CVE-2023-47875	Cross-Site Request Forgery (CSRF) vulnerability in Perfmatters allows Cross Site Request Forgery.This issue affects Perfmatters: from n/a through 2.1.6.	5.4	More Details
CVE-2023-43015	IBM InfoSphere Information Server 11.7 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: 266064.	5.4	More Details
CVE-2023-46174	IBM InfoSphere Information Server 11.7 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: 269506.	5.4	More Details
CVE-2023-4460	The Uploading SVG, WEBP and ICO files WordPress plugin through 1.2.1 does not sanitise uploaded SVG files, which could allow users with a role as low as Author to upload a malicious SVG containing XSS payloads.	5.4	More Details
CVE-2023-42009	IBM InfoSphere Information Server 11.7 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: 265504.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49283	microsoft-graph-core the Microsoft Graph Library for PHP. The Microsoft Graph Beta PHP SDK published packages which contained test code that enabled the use of the phpInfo() function from any application that could access and execute the file at `vendor/microsoft/microsoft-graph-core/tests/GetPhpInfo.php`. The phpInfo function exposes system information. The vulnerability affects the GetPhpInfo.php script of the PHP SDK which contains a call to the phpinfo() function. This vulnerability requires a misconfiguration of the server to be present so it can be exploited. For example, making the PHP application's /vendor directory web accessible. The combination of the vulnerability and the server misconfiguration would allow an attacker to craft an HTTP request that executes the phpinfo() method. The attacker would then be able to get access to system information like configuration, modules, and environment variables and later on use the compromised secrets to access additional data. This problem has been patched in version 2.0.2. If an immediate deployment with the updated vendor package is not available, you can perform the following temporary workarounds: delete the `vendor/microsoft/microsoft-graph-core/tests/GetPhpInfo.php` file, remove access to the /vendor directory, or disable the phpinfo function	5.4	More Details
CVE-2023-48866	A Cross-Site Scripting (XSS) vulnerability in the recipe preparation component within /api/objects/recipes and note component within /api/objects/shopping_lists/ of Grocy <= 4.0.3 allows attackers to obtain the victim's cookies.	5.4	More Details
CVE-2023-24050	Cross Site Scripting (XSS) vulnerability in Connectize AC21000 G6 641.139.1.1256 allows attackers to run arbitrary code via crafted string when setting the Wi-Fi password in the admin panel.	5.4	More Details
CVE-2023-44301	Dell DM5500 5.14.0.0 and prior contain a Reflected Cross-Site Scripting Vulnerability. A network attacker with low privileges could potentially exploit this vulnerability, leading to the execution of malicious HTML or JavaScript code in a victim user's web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery.	5.4	More Details
CVE-2023-6376	Henschen & Associates court document management software does not sufficiently randomize file names of cached documents, allowing a remote, unauthenticated attacker to access restricted documents.	5.3	More Details
CVE-2023-6353	Tyler Technologies Civil and Criminal Electronic Filing allows an unauthenticated, remote attacker to upload, delete, and view files by manipulating the Upload.aspx 'enky' parameter.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36523	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Gopi Ramasamy Email download link.This issue affects Email download link: from n/a through 3.7.	5.3	More Details
CVE-2023-38727	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted SQL statement. IBM X-Force ID: 262257.	5.3	More Details
CVE-2023-43021	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 266167.	5.3	More Details
CVE-2023-29258	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1, and 11.5 is vulnerable to a denial of service through a specially crafted federated query on specific federation objects. IBM X-Force ID: 252048.	5.3	More Details
CVE-2023-5915	A vulnerability of Uncontrolled Resource Consumption has been identified in STARDOM provided by Yokogawa Electric Corporation. This vulnerability may allow to a remote attacker to cause a denial-of-service condition to the FCN/FCJ controller by sending a crafted packet. While sending the packet, the maintenance homepage of the controller could not be accessed. Therefore, functions of the maintenance homepage, changing configuration, viewing logs, etc. are not available. But the controller’s operation is not stopped by the condition. The affected products and versions are as follows: STARDOM FCN/FCJ R1.01 to R4.31.	5.3	More Details
CVE-2023-3949	An issue has been discovered in GitLab affecting all versions starting from 11.3 before 16.4.3, all versions starting from 16.5 before 16.5.3, all versions starting from 16.6 before 16.6.1. It was possible for unauthorized users to view a public projects' release descriptions via an atom endpoint when release access on the public was set to only project members.	5.3	More Details
CVE-2023-6354	Tyler Technologies Magistrate Court Case Management Plus allows an unauthenticated, remote attacker to upload, delete, and view files by manipulating the PDFViewer.aspx 'filename' parameter.	5.3	More Details
CVE-2023-36507	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Repute Infosystems BookingPress – Appointment Booking Calendar Plugin and Online Scheduling Plugin.This issue affects BookingPress – Appointment Booking Calendar Plugin and Online Scheduling Plugin: from n/a through 1.0.64.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25057	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Libsyn Libsyn Publisher Hub.This issue affects Libsyn Publisher Hub: from n/a through 1.3.2.	5.3	More Details
CVE-2023-6401	A vulnerability classified as problematic was found in NotePad++ up to 8.1. Affected by this vulnerability is an unknown functionality of the file dbghelp.exe. The manipulation leads to uncontrolled search path. An attack has to be approached locally. The identifier VDB-246421 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2023-46820	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Iulia Cazan Image Regenerate & Select Crop.This issue affects Image Regenerate & Select Crop: from n/a through 7.3.0.	5.3	More Details
CVE-2023-45834	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Libsyn Libsyn Publisher Hub.This issue affects Libsyn Publisher Hub: from n/a through 1.4.4.	5.3	More Details
CVE-2023-41735	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Gopi Ramasamy Email posts to subscribers.This issue affects Email posts to subscribers: from n/a through 6.2.	5.3	More Details
CVE-2023-40662	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Jonk @ Follow me Darling Cookies and Content Security Policy.This issue affects Cookies and Content Security Policy: from n/a through 2.15.	5.3	More Details
CVE-2023-37972	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in MultiVendorX Product Stock Manager & Notifier for WooCommerce.This issue affects Product Stock Manager & Notifier for WooCommerce: from n/a through 2.0.1.	5.3	More Details
CVE-2023-6136	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Bowo Debug Log Manager.This issue affects Debug Log Manager: from n/a through 2.3.0.	5.3	More Details
CVE-2023-49948	Forgejo before 1.20.5-1 allows remote attackers to test for the existence of private user accounts by appending .rss (or another extension) to a URL.	5.3	More Details
CVE-2023-6341	Catalis (previously Icon Software) CMS360 allows a remote, unauthenticated attacker to view sensitive court documents by modifying document and other identifiers in URLs. The impact varies based on the intention and configuration of a specific CMS360 installation.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6375	Tyler Technologies Court Case Management Plus may store backups in a location that can be accessed by a remote, unauthenticated attacker. Backups may contain sensitive information such as database credentials.	5.3	More Details
CVE-2023-6342	Tyler Technologies Court Case Management Plus allows a remote attacker to authenticate as any user by manipulating at least the 'CmWebSearchPfp/Login.aspx?xyzldk=' and 'payforprint_CM/Redirector.ashx?userid=' parameters. The vulnerable "pay for print" feature was removed on or around 2023-11-01.	5.3	More Details
CVE-2023-46736	EspoCRM is an Open Source CRM (Customer Relationship Management) software. In affected versions there is Server-Side Request Forgery (SSRF) vulnerability via the upload image from url api. Users who have access to `the /Attachment/fromImageUrl` endpoint can specify URL to point to an internal host. Even though there is check for content type, it can be bypassed by redirects in some cases. This SSRF can be leveraged to disclose internal information (in some cases), target internal hosts and bypass firewalls. This vulnerability has been addressed in commit `c536cee63` which is included in release version 8.0.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2021-35975	Absolute path traversal vulnerability in the Systematica SMTP Adapter component (up to v2.0.1.101) in Systematica Radius (up to v.3.9.256.777) allows remote attackers to read arbitrary files via a full pathname in GET parameter "file" in URL. Also: affected components in same product - HTTP Adapter (up to v.1.8.0.15), MSSQL MessageBus Proxy (up to v.1.1.06), Financial Calculator (up to v.1.3.05), FIX Adapter (up to v.2.4.0.25)	5.3	More Details
CVE-2023-49082	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Improper validation makes it possible for an attacker to modify the HTTP request (e.g. insert a new header) or even create a new HTTP request if the attacker controls the HTTP method. The vulnerability occurs only if the attacker can control the HTTP method (GET, POST etc.) of the request. If the attacker can control the HTTP version of the request it will be able to modify the request (request smuggling). This issue has been patched in version 3.9.0.	5.3	More Details
CVE-2023-6180	The tokio-boring library in version 4.0.0 is affected by a memory leak issue that can lead to excessive resource consumption and potential DoS by resource exhaustion. The set_ex_data function used by the library did not deallocate memory used by pre-existing data in memory each time after completing a TLS connection causing the program to consume more resources with each new connection.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6343	Tyler Technologies Court Case Management Plus allows a remote, unauthenticated attacker to enumerate and access sensitive files using the tiffserver/tssp.aspx 'FN' and 'PN' parameters. This behavior is related to the use of a deprecated version of Aquaforest TIFF Server, possibly 2.x. The vulnerable Aquaforest TIFF Server feature was removed on or around 2023-11-01. Insecure configuration issues in Aquaforest TIFF Server are identified separately as CVE-2023-6352. CVE-2023-6343 is similar to CVE-2020-9323. CVE-2023-6343 is related to or partially caused by CVE-2023-6352.	5.3	More Details
CVE-2023-6344	Tyler Technologies Court Case Management Plus allows a remote, unauthenticated attacker to enumerate directories using the tiffserver/te003.aspx or te004.aspx 'ifolder' parameter. This behavior is related to the use of a deprecated version of Aquaforest TIFF Server, possibly 2.x. The vulnerable Aquaforest TIFF Server feature was removed on or around 2023-11-01. Insecure configuration issues in Aquaforest TIFF Server are identified separately as CVE-2023-6352. CVE-2023-6343 is related to or partially caused by CVE-2023-6352.	5.3	More Details
CVE-2023-49290	lestrrat-go/jwx is a Go module implementing various JWx (JWA/JWE/JWK/JWS/JWT, otherwise known as JOSE) technologies. A p2c parameter set too high in JWE's algorithm PBES2-* could lead to a denial of service. The JWE key management algorithms based on PBKDF2 require a JOSE Header Parameter called p2c (PBES2 Count). This parameter dictates the number of PBKDF2 iterations needed to derive a CEK wrapping key. Its primary purpose is to intentionally slow down the key derivation function, making password brute-force and dictionary attacks more resource- intensive. Therefore, if an attacker sets the p2c parameter in JWE to a very large number, it can cause a lot of computational consumption, resulting in a denial of service. This vulnerability has been addressed in commit `64f2a229b` which has been included in release version 1.2.27 and 2.0.18. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2023-6352	The default configuration of Aquaforest TIFF Server allows access to arbitrary file paths, subject to any restrictions imposed by Internet Information Services (IIS) or Microsoft Windows. Depending on how a web application uses and configures TIFF Server, a remote attacker may be able to enumerate files or directories, traverse directories, bypass authentication, or access restricted files.	5.3	More Details
CVE-2023-40687	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted RUNSTATS command on an 8TB table. IBM X-Force ID: 264809.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42574	Improper access control vulnerablility in GameHomeCN prior to version 4.2.60.2 allows local attackers to launch arbitrary activity in GameHomeCN.	5.1	More Details
CVE-2023-42559	Improper exception management vulnerability in Knox Guard prior to SMR Dec-2023 Release 1 allows Knox Guard lock bypass via changing system time.	4.9	More Details
CVE-2023-44381	October is a Content Management System (CMS) and web platform to assist with development workflow. An authenticated backend user with the `editor.cms_pages`, `editor.cms_layouts`, or `editor.cms_partials` permissions who would normally not be permitted to provide PHP code to be executed by the CMS due to `cms.safe_mode` being enabled can craft a special request to include PHP code in the CMS template. This issue has been patched in version 3.4.15.	4.9	More Details
CVE-2023-49292	ecies is an Elliptic Curve Integrated Encryption Scheme for secp256k1 in Golang. If funcations Encapsulate(), Decapsulate() and ECDH() could be called by an attacker, they could recover any private key that interacts with it. This vulnerability was patched in 2.0.8. Users are advised to upgrade.	4.9	More Details
CVE-2023-5874	The Popup box WordPress plugin before 3.8.6 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-2023-5137	The Simply Excerpts WordPress plugin through 1.4 does not sanitize and escape some fields in the plugin settings, which could allow high-privilege users such as an administrator to inject arbitrary web scripts even when the unfiltered_html capability is disallowed (for example in a multisite setup).	4.8	More Details
CVE-2023-5226	An issue has been discovered in GitLab affecting all versions before 16.4.3, all versions starting from 16.5 before 16.5.3, all versions starting from 16.6 before 16.6.1. Under certain circumstances, a malicious actor bypass prohibited branch checks using a specially crafted branch name to manipulate repository content in the UI.	4.8	More Details
CVE-2023-48880	A stored cross-site scripting (XSS) vulnerability in EyouCMS v1.6.4-UTF8-SP1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Menu Name field at /login.php?m=admin&c=Index&a=changeTableVal&_ajax=1&lang=cn.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48881	A stored cross-site scripting (XSS) vulnerability in EyouCMS v1.6.4-UTF8-SP1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Field Title field at /login.php?m=admin&c=Field&a=arctype_add&_ajax=1&lang=cn.	4.8	More Details
CVE-2023-48882	A stored cross-site scripting (XSS) vulnerability in EyouCMS v1.6.4-UTF8-SP1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Document Properties field at /login.php m=admin&c=Index&a=changeTableVal&_ajax=1&lang=cn.	4.8	More Details
CVE-2023-46746	PostHog provides open-source product analytics, session recording, feature flagging and A/B testing that you can self-host. A server-side request forgery (SSRF), which can only be exploited by authenticated users, was found in Posthog. Posthog did not verify whether a URL was local when enabling webhooks, allowing authenticated users to forge a POST request. This vulnerability has been addressed in `22bd5942` and will be included in subsequent releases. There are no known workarounds for this vulnerability.	4.8	More Details
CVE-2023-47106	Traefik is an open source HTTP reverse proxy and load balancer. When a request is sent to Traefik with a URL fragment, Traefik automatically URL encodes and forwards the fragment to the backend server. This violates RFC 7230 because in the origin-form the URL should only contain the absolute path and the query. When this is combined with another frontend proxy like Nginx, it can be used to bypass frontend proxy URI-based access control restrictions. This vulnerability has been addressed in versions 2.10.6 and 3.0.0-beta5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.8	More Details
CVE-2023-5809	The Popup box WordPress plugin before 3.8.6 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-2021-36806	A reflected XSS vulnerability allows an open redirect when the victim clicks a malicious link to an error page on Sophos Email Appliance older than version 4.5.3.4.	4.7	More Details
CVE-2023-49281	Calendarinho is an open source calendaring application to manage large teams of consultants. An Open Redirect issue occurs when a web application redirects users to external URLs without proper validation. This can lead to phishing attacks, where users are tricked into visiting malicious sites, potentially leading to information theft and reputational damage to the website used for redirection. The problem is has been patched in commit `15b2393`. Users are advised to update to a commit after `15b2393`. There are no known workarounds for this vulnerability.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42573	PendingIntent hijacking vulnerability in Search Widget prior to version 3.4 in China models allows local attackers to access data.	4.7	More Details
CVE-2023-34390	An input validation vulnerability in the Schweitzer Engineering Laboratories SEL-451 could allow a remote authenticated attacker to create a denial of service against the system and locking out services. See product Instruction Manual Appendix A dated 20230830 for more details.	4.5	More Details
CVE-2023-34389	An allocation of resources without limits or throttling vulnerability in the Schweitzer Engineering Laboratories SEL-451 could allow a remote authenticated attacker to make the system unavailable for an indefinite amount of time. See product Instruction Manual Appendix A dated 20230830 for more details.	4.5	More Details
CVE-2023-32856	In display, there is a possible out of bounds read due to an incorrect status check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07993705; Issue ID: ALPS07993705.	4.4	More Details
CVE-2023-42680	In gpu driver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-32858	In GZ, there is a possible information disclosure due to a missing data erasing. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07806008; Issue ID: ALPS07806008.	4.4	More Details
CVE-2023-32857	In display, there is a possible out of bounds read due to an incorrect status check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07993705; Issue ID: ALPS07993710.	4.4	More Details
CVE-2023-42682	In gsp driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-32852	In cameraisp, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07670971; Issue ID: ALPS07670971.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42726	In TeleService, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-42731	In Gnss service, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-42729	In ril service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-42735	In telephony service, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed	4.4	More Details
CVE-2023-42751	In gnss service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-5995	An issue has been discovered in GitLab EE affecting all versions starting from 16.2 before 16.4.3, all versions starting from 16.5 before 16.5.3, all versions starting from 16.6 before 16.6.1. It was possible for an attacker to abuse the policy bot to gain access to internal projects.	4.4	More Details
CVE-2023-42727	In gpu driver, there is a possible out of bounds write due to a incorrect bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-42725	In gpu driver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-42724	In gpu driver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-42684	In gsp driver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-42683	In gsp driver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43089	Dell Rugged Control Center, version prior to 4.7, contains insufficient protection for the Policy folder. A local malicious standard user could potentially exploit this vulnerability to modify the content of the policy file, leading to unauthorized access to resources.	4.4	More Details
CVE-2023-42679	In gpu driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-48323	Cross-Site Request Forgery (CSRF) vulnerability in Awesome Support Team Awesome Support – WordPress HelpDesk & Support Plugin allows Cross Site Request Forgery.This issue affects Awesome Support – WordPress HelpDesk & Support Plugin: from n/a through 6.1.4.	4.3	More Details
CVE-2023-36685	Cross-Site Request Forgery (CSRF) vulnerability in Brainstorm Force US LLC CartFlows Pro allows Cross Site Request Forgery.This issue affects CartFlows Pro: from n/a through 1.11.12.	4.3	More Details
CVE-2023-47645	Cross-Site Request Forgery (CSRF) vulnerability in RegistrationMagic RegistrationMagic – Custom Registration Forms, User Registration, Payment, and User Login allows Cross Site Request Forgery.This issue affects RegistrationMagic – Custom Registration Forms, User Registration, Payment, and User Login: from n/a through 5.2.2.6.	4.3	More Details
CVE-2022-24403	The TETRA TA61 identity encryption function internally uses a 64-bit value derived exclusively from the SCK (Class 2 networks) or CCK (Class 3 networks). The structure of TA61 allows for efficient recovery of this 64-bit value, allowing an adversary to encrypt or decrypt arbitrary identities given only three known encrypted/unencrypted identity pairs.	4.3	More Details
CVE-2023-48331	Cross-Site Request Forgery (CSRF) vulnerability in Stormhill Media MyBookTable Bookstore by Stormhill Media allows Cross Site Request Forgery.This issue affects MyBookTable Bookstore by Stormhill Media: from n/a through 3.3.4.	4.3	More Details
CVE-2023-49094	Symbolicator is a symbolication service for native stacktraces and minidumps with symbol server support. An attacker could make Symbolicator send arbitrary GET HTTP requests to internal IP addresses by using a specially crafted HTTP endpoint. The response could be reflected to the attacker if they have an account on Sentry instance. The issue has been fixed in the release 23.11.2.	4.3	More Details
CVE-2023-48284	Cross-Site Request Forgery (CSRF) vulnerability in WebToffee Decorator – WooCommerce Email Customizer allows Cross Site Request Forgery.This issue affects Decorator – WooCommerce Email Customizer: from n/a through 1.2.7.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48283	Cross-Site Request Forgery (CSRF) vulnerability in PressTigers Simple Testimonials Showcase allows Cross Site Request Forgery.This issue affects Simple Testimonials Showcase: from n/a through 1.1.5.	4.3	More Details
CVE-2023-49076	Customer-data-framework allows management of customer data within Pimcore. There are no tokens or headers to prevent CSRF attacks from occurring, therefore an attacker could abuse this vulnerability to create new customers. This issue has been patched in version 4.0.5.	4.3	More Details
CVE-2023-6474	A vulnerability has been found in PHPGurukul Nipah Virus Testing Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file manage-phlebotomist.php. The manipulation of the argument pid leads to cross-site request forgery. 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-246640.	4.3	More Details
CVE-2023-5772	The Debug Log Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.2.1. This is due to missing or incorrect nonce validation on the clear_log() function. This makes it possible for unauthenticated attackers to clear the debug log via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-49674	A missing permission check in Jenkins NeuVector Vulnerability Scanner Plugin 1.22 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified hostname and port using attacker-specified username and password.	4.3	More Details
CVE-2023-6070	A server-side request forgery vulnerability in ESM prior to version 11.6.8 allows a low privileged authenticated user to upload arbitrary content, potentially altering configuration. This is possible through the certificate validation functionality where the API accepts uploaded content and doesn't parse for invalid data	4.3	More Details
CVE-2023-48281	Cross-Site Request Forgery (CSRF) vulnerability in Super Blog Me Broken Link Checker for YouTube allows Cross Site Request Forgery.This issue affects Broken Link Checker for YouTube: from n/a through 1.3.	4.3	More Details
CVE-2023-48279	Cross-Site Request Forgery (CSRF) vulnerability in Seraphinite Solutions Seraphinite Post .DOCX Source allows Cross Site Request Forgery.This issue affects Seraphinite Post .DOCX Source: from n/a through 2.16.6.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31177	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in the Schweitzer Engineering Laboratories SEL-451 could allow an attacker to craft a link that could execute arbitrary code on a victim's system. See product Instruction Manual Appendix A dated 20230830 for more details.	4.3	More Details
CVE-2023-48328	Cross-Site Request Forgery (CSRF) vulnerability in Imagely WordPress Gallery Plugin – NextGEN Gallery allows Cross Site Request Forgery.This issue affects WordPress Gallery Plugin – NextGEN Gallery: from n/a through 3.37.	4.3	More Details
CVE-2023-2267	An Improper Input Validation vulnerability in Schweitzer Engineering Laboratories SEL-411L could allow an attacker to perform reflection attacks against an authorized and authenticated user. See product Instruction Manual Appendix A dated 20230830 for more details.	4.3	More Details
CVE-2023-2266	An Improper neutralization of input during web page generation in the Schweitzer Engineering Laboratories SEL-411L could allow an attacker to generate cross-site scripting based attacks against an authorized and authenticated user. See product Instruction Manual Appendix A dated 20230830 for more details.	4.3	More Details
CVE-2023-2265	An Improper Restriction of Rendered UI Layers or Frames in the Schweitzer Engineering Laboratories SEL-411L could allow an unauthenticated attacker to perform clickjacking based attacks against an authenticated and authorized user. See product Instruction Manual Appendix A dated 20230830 for more details.	4.3	More Details
CVE-2023-5803	Cross-Site Request Forgery (CSRF) vulnerability in Business Directory Team Business Directory Plugin – Easy Listing Directories for WordPress allows Cross-Site Request Forgery.This issue affects Business Directory Plugin – Easy Listing Directories for WordPress: from n/a through 6.3.10.	4.3	More Details
CVE-2023-38268	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 260585.	4.3	More Details
CVE-2023-37890	Missing Authorization vulnerability in WPOmnia KB Support – WordPress Help Desk and Knowledge Base allows Accessing Functionality Not Properly Constrained by ACLs. Users with a role as low as a subscriber can view other customers.This issue affects KB Support – WordPress Help Desk and Knowledge Base: from n/a through 1.5.88.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3964	An issue has been discovered in GitLab affecting all versions starting from 13.2 before 16.4.3, all versions starting from 16.5 before 16.5.3, all versions starting from 16.6 before 16.6.1. It was possible for users to access composer packages on public projects that have package registry disabled in the project settings.	4.3	More Details
CVE-2023-6438	A vulnerability classified as problematic has been found in Thecosy IceCMS 2.0.1. Affected is an unknown function of the file /WebArticle/articles/ of the component Like Handler. The manipulation leads to improper enforcement of a single, unique action. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-246438 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2023-6465	A vulnerability was found in PHPGurukul Nipah Virus Testing Management System 1.0. It has been classified as problematic. This affects an unknown part of the file registered-user-testing.php. The manipulation of the argument regmobilenumber 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-246615.	4.3	More Details
CVE-2023-4317	An issue has been discovered in GitLab affecting all versions starting from 9.2 before 16.4.3, all versions starting from 16.5 before 16.5.3, all versions starting from 16.6 before 16.6.1. It was possible for a user with the Developer role to update a pipeline schedule from an unprotected branch to a protected branch.	4.3	More Details
CVE-2023-45083	An Improper Privilege Management vulnerability exists in HyperCloud that will impact the ability for a user to authenticate against the management plane. An authenticated admin-level user may be able to delete the "admin" or "serveradmin" users, which prevents authentication from subsequently succeeding. This issue affects HyperCloud versions 1.0 to any release before 2.1.	4.2	More Details
CVE-2023-42569	Improper authorization verification vulnerability in AR Emoji prior to SMR Dec-2023 Release 1 allows attackers to read sandbox data of AR Emoji.	4.0	More Details
CVE-2023-6460	A potential logging of the firestore key via logging within nodejs-firestore exists - Developers who were logging objects through this._settings would be logging the firestore key as well potentially exposing it to anyone with logs read access. We recommend upgrading to version 6.1.0 to avoid this issue	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2264	An improper input validation vulnerability in the Schweitzer Engineering Laboratories SEL-411L could allow a malicious actor to manipulate authorized users to click on a link that could allow undesired behavior. See product Instruction Manual Appendix A dated 20230830 for more details.	4.0	More Details
CVE-2023-49284	fish is a smart and user-friendly command line shell for macOS, Linux, and the rest of the family. fish shell uses certain Unicode non-characters internally for marking wildcards and expansions. It will incorrectly allow these markers to be read on command substitution output, rather than transforming them into a safe internal representation. While this may cause unexpected behavior with direct input (for example, echo \UFDD2HOME has the same output as echo $HOME), this may become a minor security problem if the output is being fed from an external program into a command substitution where this output may not be expected. This design flaw was introduced in very early versions of fish, predating the version control system, and is thought to be present in every version of fish released in the last 15 years or more, although with different characters. Code execution does not appear to be possible, but denial of service (through large brace expansion) or information disclosure (such as variable expansion) is potentially possible under certain circumstances. fish shell 3.6.2 has been released to correct this issue. Users are advised to upgrade. There are no known workarounds for this vulnerability.	3.9	More Details
CVE-2023-37867	Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in YetAnotherStarsRating.Com YASR – Yet Another Star Rating Plugin for WordPress.This issue affects YASR – Yet Another Star Rating Plugin for WordPress: from n/a through 3.3.8.	3.7	More Details
CVE-2023-44298	Dell PowerEdge platforms 16G Intel E5 BIOS and Dell Precision BIOS, version 1.4.4, contain active debug code security vulnerability. An unauthenticated physical attacker could potentially exploit this vulnerability, leading to information tampering, code execution, denial of service.	3.6	More Details
CVE-2023-28895	The password for access to the debugging console of the PoWer Controller chip (PWC) of the MIB3 infotainment is hard-coded in the firmware. The console allows attackers with physical access to the MIB3 unit to gain full control over the PWC chip. Vulnerability found on Škoda Superb III (3V3) - 2.0 TDI manufactured in 2022.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6442	A vulnerability was found in PHPGurukul Nipah Virus Testing Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file add-phlebotomist.php. The manipulation of the argument empid/fullname 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-246445 was assigned to this vulnerability.	3.5	More Details
CVE-2023-6440	A vulnerability was found in SourceCodester Book Borrower System 1.0 and classified as problematic. This issue affects some unknown processing of the file endpoint/add-book.php. The manipulation of the argument Book Title/Book Author 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-246443.	3.5	More Details
CVE-2023-6466	A vulnerability was found in Thecosy IceCMS 2.0.1. It has been declared as problematic. This vulnerability affects unknown code of the file /planet of the component User Comment Handler. The manipulation leads to cross site scripting. 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-246616.	3.5	More Details
CVE-2023-6439	A vulnerability classified as problematic was found in ZenTao PMS 18.8. Affected by this vulnerability is an unknown functionality. 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 associated identifier of this vulnerability is VDB-246439.	3.5	More Details
CVE-2023-49080	The Jupyter Server provides the backend (i.e. the core services, APIs, and REST endpoints) for Jupyter web applications like Jupyter notebook, JupyterLab, and Voila. Unhandled errors in API requests coming from an authenticated user include traceback information, which can include path information. There is no known mechanism by which to trigger these errors without authentication, so the paths revealed are not considered particularly sensitive, given that the requesting user has arbitrary execution permissions already in the same environment. A fix has been introduced in commit `0056c3aa52` which no longer includes traceback information in JSON error responses. For compatibility, the traceback field is present, but always empty. This commit has been included in version 2.11.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6473	A vulnerability, which was classified as problematic, was found in SourceCodester Online Quiz System 1.0. This affects an unknown part of the file take-quiz.php. The manipulation of the argument quiz_taker/year_section 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-246639.	3.5	More Details
CVE-2018-25094	A vulnerability was found in ระบบบัญชีออนไลน์ Online Accounting System up to 1.4.0 and classified as problematic. This issue affects some unknown processing of the file ckeditor/filemanager/browser/default/image.php. The manipulation of the argument fid with the input ../../../etc/passwd leads to path traversal: '../filedir'. The exploit has been disclosed to the public and may be used. Upgrading to version 2.0.0 is able to address this issue. The identifier of the patch is 9d9618422b980335bb30be612ea90f4f56cb992c. It is recommended to upgrade the affected component. The identifier VDB-246641 was assigned to this vulnerability.	3.5	More Details
CVE-2023-6463	A vulnerability has been found in SourceCodester User Registration and Login System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /endpoint/add-user.php. The manipulation of the argument first_name 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-246613 was assigned to this vulnerability.	3.5	More Details
CVE-2023-6462	A vulnerability, which was classified as problematic, was found in SourceCodester User Registration and Login System 1.0. Affected is an unknown function of the file /endpoint/delete-user.php. The manipulation of the argument user 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-246612.	3.5	More Details
CVE-2022-4957	A vulnerability was found in librespeed speedtest up to 5.2.4. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file results/stats.php. The manipulation of the argument id leads to cross site scripting. The attack can be launched remotely. Upgrading to version 5.2.5 is able to address this issue. The patch is named a85f2c086f3449dffa8fe2edb5e2ef3ee72dc0e9. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-246643.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49297	PyDrive2 is a wrapper library of google-api-python-client that simplifies many common Google Drive API V2 tasks. Unsafe YAML deserilization will result in arbitrary code execution. A maliciously crafted YAML file can cause arbitrary code execution if PyDrive2 is run in the same directory as it, or if it is loaded in via `LoadSettingsFile`. This is a deserilization attack that will affect any user who initializes GoogleAuth from this package while a malicious yaml file is present in the same directory. This vulnerability does not require the file to be directly loaded through the code, only present. This issue has been addressed in commit `c57355dc` which is included in release version `1.16.2`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	3.3	More Details
CVE-2023-42556	Improper usage of implicit intent in Contacts prior to SMR Dec-2023 Release 1 allows attacker to get sensitive information.	3.3	More Details
CVE-2023-42572	Implicit intent hijacking vulnerability in Samsung Account Web SDK prior to version 1.5.24 allows attacker to get sensitive information.	3.3	More Details
CVE-2023-28896	Access to critical Unified Diagnostics Services (UDS) of the Modular Infotainment Platform 3 (MIB3) infotainment is transmitted via Controller Area Network (CAN) bus in a form that can be easily decoded by attackers with physical access to the vehicle. Vulnerability discovered on Škoda Superb III (3V3) - 2.0 TDI manufactured in 2022.	3.3	More Details
CVE-2023-45085	An issue exists in SoftIron HyperCloud where compute nodes may come online immediately without following the correct initialization process. In this instance, workloads may be scheduled on these nodes and deploy to a failed or erroneous state, which impacts the availability of these workloads that may be deployed during this time window. This issue impacts HyperCloud versions from 2.0.0 to before 2.0.3.	3.2	More Details
CVE-2023-6467	A vulnerability was found in Thecosy IceCMS 2.0.1. It has been rated as problematic. This issue affects some unknown processing of the file /Websquare/likeClickComment/ of the component Comment Like Handler. The manipulation leads to improper enforcement of a single, unique action. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-246617 was assigned to this vulnerability.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4658	An issue has been discovered in GitLab EE affecting all versions starting from 8.13 before 16.4.3, all versions starting from 16.5 before 16.5.3, all versions starting from 16.6 before 16.6.1. It was possible for an attacker to abuse the `Allowed to merge` permission as a guest user, when granted the permission through a group.	3.1	More Details
CVE-2023-3443	An issue has been discovered in GitLab affecting all versions starting from 12.1 before 16.4.3, all versions starting from 16.5 before 16.5.3, all versions starting from 16.6 before 16.6.1. It was possible for a Guest user to add an emoji on confidential work items.	3.1	More Details
CVE-2023-49652	Incorrect permission checks in Jenkins Google Compute Engine Plugin 4.550.vb_327fca_3db_11 and earlier allow attackers with global Item/Configure permission (while lacking Item/Configure permission on any particular job) to enumerate system-scoped credentials IDs of credentials stored in Jenkins and to connect to Google Cloud Platform using attacker-specified credentials IDs obtained through another method, to obtain information about existing projects. This fix has been backported to 4.3.17.1.	2.7	More Details
CVE-2023-4912	An issue has been discovered in GitLab EE affecting all versions starting from 10.5 before 16.4.3, all versions starting from 16.5 before 16.5.3, all versions starting from 16.6 before 16.6.1. It was possible for an attacker to cause a client-side denial of service using malicious crafted mermaid diagram input.	2.6	More Details
CVE-2023-5274	Improper Input Validation vulnerability in simulation function of GX Works2 allows an attacker to cause a denial-of-service (DoS) condition on the function by sending specially crafted packets. However, the attacker would need to send the packets from within the same personal computer where the function is running.	2.5	More Details
CVE-2023-5275	Improper Input Validation vulnerability in simulation function of GX Works2 allows an attacker to cause a denial-of-service (DoS) condition on the function by sending specially crafted packets. However, the attacker would need to send the packets from within the same personal computer where the function is running.	2.5	More Details
CVE-2023-6472	A vulnerability, which was classified as problematic, has been found in PHPEMS 7.0. This issue affects some unknown processing of the file app\content\cls\api.cls.php of the component Content Section Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-246629 was assigned to this vulnerability.	2.4	More Details