IBLISS DIGITAL SECURITY

Vulnerabilidades Publicadas Na Semana

Vulnerabilidades de Severidade Crítica

ID	CVSS Score	Descrição	Publicado em	Última Modificação
CVE-2023-1267	9.8	"Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ulkem Company PtteM Kart.This issue affects PtteM Kart: before 2.1."	2023-03-08T12:15:09.267	2023-03-14T19:12:58.583
CVE-2023-25395	9.8	'TOTOlink A7100RU V7.4cu.2313_B20191024 router has a command injection vulnerability.	2023-03-08T14:15:09.760	2023-03-14T18:58:20.090
CVE-2023-26261	9.8	'In UBIKA WAAP Gateway/Cloud through 6.10, a blind XPath injection leads to an authentication bypass by stealing the session of another connected user. The fixed versions are WAAP Gateway & Cloud 6.11.0 and 6.5.6-patch15.	2023-03-08T15:15:10.473	2023-03-15T13:43:29.197
CVE-2023-24773	9.8	'Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the id parameter at /databases/database/list.	2023-03-08T16:15:09.403	2023-03-14T16:48:04.363
CVE-2023-26922	9.8	'SQL injection vulnerability found in Varisicte matrix-gui v.2 allows a remote attacker to execute arbitrary code via the shell_exect parameter to the \\www\\pages\\matrix-gui-2.0 endpoint.	2023-03-08T16:15:09.470	2023-03-14T15:34:47.473

CVE-2023-27482	10.0	'homeassistant is an open source home automation tool. A remotely exploitable vulnerability bypassing authentication for accessing the Supervisor API through Home Assistant has been discovered. This impacts all Home Assistant installation types that use the Supervisor 2023.01.1 or older. Installation types, like Home Assistant Container (for example Docker), or Home Assistant Core manually in a Python environment, are not affected. The issue has been mitigated and closed in Supervisor version 2023.03.1, which has been rolled out to all affected installations via the auto-update feature of the Supervisor. This rollout has been completed at the time of publication of this advisory. Home Assistant Core 2023.3.0 included mitigation for this vulnerability. Upgrading to at least that version is thus advised. In case one is not able to upgrade the Home Assistant Supervisor or the Home Assistant Core application at this time, it is advised to not expose your Home Assistant instance to the internet.	2023-03-08T18:15:11.783	2023-03-15T14:20:39.313
CVE-2023-26489	9.9	"wasmtime is a fast and secure runtime for WebAssembly. In affected versions wasmtime's code generator, Cranelift, has a bug on x86_64 targets where address-mode computation mistakenly would calculate a 35-bit effective address instead of WebAssembly's defined 33-bit effective address. This bug means that, with default codegen settings, a wasm-controlled load/store operation could read/write addresses up to 35 bits away from the base of linear memory. Due to this bug, however, addresses up to `0xffffffff * 8 + 0x7ffffffc = 36507222004 = ~34G` bytes away from the base of linear memory are possible from guest code. This means that the virtual memory 6G away from the base of linear memory up to ~34G away can be read/written by a malicious module. A guest module can, without the knowledge of the embedder, read/write memory in this region. The memory may belong to other WebAssembly instances when using the pooling allocator, for example. Affected embedders are recommended to analyze preexisting wasm modules to see if they're affected by the incorrect codegen rules and possibly correlate that with an anomalous number of traps during historical execution to locate possibly suspicious modules. The specific bug in Cranelift's x86_64 backend is that a WebAssembly address which is left-shifted by a constant amount from 1 to 3 will get folded into x86_64's addressing modes which perform shifts. For example `(i32.load (i32.shl (local.get 0) (i32.const 3)))` loads from the WebAssembly address `$local0 << 3`. When translated to Cranelift the `$local0 << 3` computation, a 32-bit value, is zero-extended to a 64-bit value and then added to the base address of linear memory. Cranelift would generate an instruction of the form `movl (%base, %local0, 8), %dst` which calculates `%base + %local0 << 3`. The bug here, however, is that the address computation happens with 64-bit values, where the `$local0 << 3` computation was supposed to be truncated to a a 32-bit value. This means that `%local0`, which can use up to 32-bits for an address, gets 3 extra bits of address space to be accessible via this `movl` instruction. The fix in Cranelift	2023-03-08T20:15:09.583	2023-03-09T14:01:48.500

		is to remove the erroneous lowering rules in the backend which handle these zero-extended expression. The above example is then translated to `movl %local0, %temp; shl $3, %temp; movl (%base, %temp), %dst` which correctly truncates the intermediate computation of `%local0 << 3` to 32-bits inside the `%temp` register which is then added to the `%base` value. Wasmtime version 4.0.1, 5.0.1, and 6.0.1 have been released and have all been patched to no longer contain the erroneous lowering rules. While updating Wasmtime is recommended, there are a number of possible workarounds that embedders can employ to mitigate this issue if updating is not possible. Note that none of these workarounds are on-by-default and require explicit configuration: 1. The `Config::static_memory_maximum_size(0)` option can be used to force all accesses to linear memory to be explicitly bounds-checked. This will perform a bounds check separately from the address-mode computation which correctly calculates the effective address of a load/store. Note that this can have a large impact on the execution performance of WebAssembly modules. 2. The `Config::static_memory_guard_size(1 << 36)` option can be used to greatly increase the guard pages placed after linear memory. This will guarantee that memory accesses up-to-34G away are guaranteed to be semantically correct by reserving unmapped memory for the instance. Note that this reserves a very large amount of virtual memory per-instances and can greatly reduce the maximum number of concurrent instances being run. 3. If using a non-x86_64 host is possible, then that will also work around this bug. This bug does not affect Wasmtime's or Cranelift's AArch64 backend, for example."		
CVE-2023-22889	9.8	'SmartBear Zephyr Enterprise through 7.15.0 mishandles user-defined input during report generation. This could lead to remote code execution by unauthenticated users.	2023-03-08T21:15:10.643	2023-03-14T19:37:28.607
CVE-2023-24782	9.8	'Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the id parameter at /databases/database/edit.	2023-03-08T21:15:10.943	2023-03-14T16:58:12.273
CVE-2021-33351	9.0	'Cross Site Scripting Vulnerability in Wyomind Help Desk Magento 2 extension v.1.3.6 and before and fixed in v.1.3.7 allows attackers to escalte privileges via a crafted payload in the ticket message field.	2023-03-08T22:15:09.480	2023-03-14T20:09:57.310
CVE-2021-33352	9.8	'An issue in Wyomind Help Desk Magento 2 extension v.1.3.6 and before fixed in v.1.3.7 allows attacker to execute arbitrary code via a phar file upload in the ticket message field.	2023-03-08T22:15:09.537	2023-03-14T20:13:39.207
CVE-2021-33353	9.8	'Directory Traversal vulnerability in Wyomind Help Desk Magento 2 extension v.1.3.6 and before fixed in v.1.3.7 allows attacker to execute arbitrary code via the file attachment directory setting.	2023-03-08T22:15:09.593	2023-03-14T20:05:20.493
CVE-2023-1283	10.0	'Code Injection in GitHub repository builderio/qwik prior to 0.21.0.	2023-03-08T22:15:09.683	2023-03-14T19:39:32.307

CVE-2023-24777	9.8	'Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the id parameter at /databases/table/list.	2023-03-08T22:15:09.797	2023-03-14T16:58:30.177
CVE-2023-27985	9.8	'emacsclient-mail.desktop in Emacs 28.1 through 28.2 is vulnerable to shell command injections through a crafted mailto: URI. This is related to lack of compliance with the Desktop Entry Specification.	2023-03-09T06:15:32.987	2023-03-15T13:48:33.450
CVE-2023-27986	9.8	'emacsclient-mail.desktop in Emacs 28.1 through 28.2 is vulnerable to Emacs Lisp code injections through a crafted mailto: URI with unescaped double-quote characters.	2023-03-09T06:15:33.187	2023-03-15T13:49:50.633
CVE-2023-1251	9.8	"Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Akinsoft Wolvox. This issue affects Wolvox: before 8.02.03."	2023-03-09T08:15:08.553	2023-03-09T14:01:48.500
CVE-2023-1291	6.3	'A vulnerability, which was classified as critical, was found in SourceCodester Sales Tracker Management System 1.0. This affects an unknown part of the file admin/clients/manage_client.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222645 was assigned to this vulnerability.	2023-03-09T15:15:09.217	2023-03-15T13:40:29.353
CVE-2023-1292	6.3	'A vulnerability has been found in SourceCodester Sales Tracker Management System 1.0 and classified as critical. This vulnerability affects the function delete_client of the file classes/Master.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-222646 is the identifier assigned to this vulnerability.	2023-03-09T15:15:09.307	2023-03-15T13:36:47.247
CVE-2023-1294	7.3	'A vulnerability was found in SourceCodester File Tracker Manager System 1.0. It has been classified as critical. Affected is an unknown function of the file /file_manager/login.php of the component POST Parameter Handler. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222648.	2023-03-09T15:15:09.517	2023-03-15T13:33:38.893
CVE-2023-1287	9.0	'An XSL template vulnerability in ENOVIA Live Collaboration V6R2013xE allows Remote Code Execution.	2023-03-09T17:15:10.240	2023-03-09T20:03:55.143
CVE-2023-26957	9.1	'onekeyadmin v1.3.9 was discovered to contain an arbitrary file delete vulnerability via the component \\admin\\controller\\plugins.	2023-03-09T21:15:10.963	2023-03-15T14:53:39.940
CVE-2023-27202	9.8	'Best POS Management System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /kruxton/receipt.php.	2023-03-09T21:15:11.027	2023-03-13T03:51:33.370

CVE-2023-27203	9.8	'Best POS Management System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /billing/home.php.	2023-03-09T21:15:11.080	2023-03-13T03:51:39.573
CVE-2023-27204	9.8	'Best POS Management System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /kruxton/manage_user.php.	2023-03-09T21:15:11.140	2023-03-13T03:51:44.600
CVE-2023-27205	9.8	'Best POS Management System 1.0 was discovered to contain a SQL injection vulnerability via the month parameter at /kruxton/sales_report.php.	2023-03-09T21:15:11.197	2023-03-13T03:51:52.557
CVE-2023-27207	9.8	'Online Pizza Ordering System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/manage_user.php.	2023-03-09T21:15:11.317	2023-03-13T03:51:59.073
CVE-2023-27210	9.8	'Online Pizza Ordering System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/view_order.php.	2023-03-09T21:15:11.437	2023-03-13T03:52:04.883
CVE-2023-27213	9.8	'Online Student Management System v1.0 was discovered to contain a SQL injection vulnerability via the searchdata parameter at /eduauth/student/search.php.	2023-03-09T21:15:11.607	2023-03-13T03:52:12.113
CVE-2023-27214	9.8	'Online Student Management System v1.0 was discovered to contain multiple SQL injection vulnerabilities via the fromdate and todate parameters at /eduauth/student/between-date-reprtsdetails.php.	2023-03-09T21:15:11.663	2023-03-13T03:52:17.803
CVE-2023-1300	6.3	'A vulnerability classified as critical was found in SourceCodester COVID 19 Testing Management System 1.0. Affected by this vulnerability is an unknown functionality of the file patient-report.php of the component POST Parameter Handler. The manipulation of the argument searchdata leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222661 was assigned to this vulnerability.	2023-03-09T22:15:51.880	2023-03-14T16:07:26.273
CVE-2023-1301	6.3	'A vulnerability, which was classified as critical, has been found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. Affected by this issue is some unknown functionality of the file deleteorder.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-222662 is the identifier assigned to this vulnerability.	2023-03-09T22:15:51.957	2023-03-14T16:36:37.887
CVE-2023-1307	9.8	'Authentication Bypass by Primary Weakness in GitHub repository froxlor/froxlor prior to 2.0.13.	2023-03-10T01:15:11.927	2023-03-10T13:53:24.757
CVE-2023-1091	10.0	"Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Alpata Licensed Warehousing Automation System allows Command Line Execution through SQL Injection.This issue affects Licensed Warehousing Automation System: through 2023.1.01."	2023-03-10T08:15:09.610	2023-03-10T13:53:17.070

CVE-2023-1308	6.3	'A vulnerability classified as critical has been found in SourceCodester Online Graduate Tracer System 1.0. Affected is an unknown function of the file admin/adminlog.php. The manipulation of the argument user leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222696.	2023-03-10T08:15:09.997	2023-03-14T16:46:11.107
CVE-2023-1309	6.3	'A vulnerability classified as critical was found in SourceCodester Online Graduate Tracer System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/search_it.php. The manipulation of the argument input leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222697 was assigned to this vulnerability.	2023-03-10T08:15:10.123	2023-03-14T16:46:26.460
CVE-2023-1310	6.3	'A vulnerability, which was classified as critical, has been found in SourceCodester Online Graduate Tracer System 1.0. Affected by this issue is some unknown functionality of the file admin/prof.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-222698 is the identifier assigned to this vulnerability.	2023-03-10T08:15:10.300	2023-03-14T16:46:35.450
CVE-2023-1311	6.3	'A vulnerability, which was classified as critical, was found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. This affects an unknown part of the file large.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222699.	2023-03-10T08:15:10.407	2023-03-14T16:46:55.090
CVE-2021-33360	9.8	'An issue found in Stoqey gnuplot v.0.0.3 and earlier allows attackers to execute arbitrary code via the src/index.ts, plotCallack, child_process, and/or filePath parameter(s).	2023-03-10T16:15:10.427	2023-03-15T13:48:40.177
CVE-2022-33256	9.8	'Memory corruption due to improper validation of array index in Multi-mode call processor.	2023-03-10T21:15:11.897	2023-03-11T02:54:29.333
CVE-2022-33257	9.3	'Memory corruption in Core due to time-of-check time-of-use race condition during dump collection in trust zone.	2023-03-10T21:15:11.963	2023-03-11T02:54:29.333
CVE-2023-1198	9.8	"Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Saysis Starcities allows SQL Injection.This issue affects Starcities: through 1.3."	2023-03-10T21:15:14.550	2023-03-11T02:54:29.333
CVE-2022-38074	9.9	'SQL Injection vulnerability in VeronaLabs WP Statistics plugin <= 13.2.10 versions.	2023-03-13T14:15:12.627	2023-03-13T14:48:34.443
CVE-2023-0345	9.8	'The Akuvox E11 secure shell (SSH) server is enabled by default and can be accessed by the root user. This password cannot be changed by the user.	2023-03-13T21:15:13.010	2023-03-14T13:33:10.470

CVE-2023-0352	9.1	'The Akuvox E11 password recovery webpage can be accessed without authentication, and an attacker could download the device key file. An attacker could then use this page to reset the password back to the default.	2023-03-13T21:15:13.653	2023-03-14T13:33:10.470
CVE-2023-0354	9.1	'The Akuvox E11 web server can be accessed without any user authentication, and this could allow an attacker to access sensitive information, as well as create and download packet captures with known default URLs.	2023-03-13T21:15:13.893	2023-03-14T13:33:10.470
CVE-2023-27583	9.8	'PanIndex is a network disk directory index. In Panindex prior to version 3.1.3, a hard-coded JWT key `PanIndex` is used. An attacker can use the hard-coded JWT key to sign JWT token and perform any actions as a user with admin privileges. Version 3.1.3 has a patch for the issue. As a workaround, one may change the JWT key in the source code before compiling the project.	2023-03-13T21:15:14.130	2023-03-14T13:33:10.470
CVE-2023-27582	9.1	'maddy is a composable, all-in-one mail server. Starting with version 0.2.0 and prior to version 0.6.3, maddy allows a full authentication bypass if SASL authorization username is specified when using the PLAIN authentication mechanisms. Instead of validating the specified username, it is accepted as is after checking the credentials for the authentication username. maddy 0.6.3 includes the fix for the bug. There are no known workarounds.	2023-03-13T22:15:12.387	2023-03-14T13:33:10.470
CVE-2023-23857	9.9	'Due to missing authentication check, SAP NetWeaver AS for Java - version 7.50, allows an unauthenticated attacker to attach to an open interface and make use of an open naming and directory API to access services which can be used to perform unauthorized operations affecting users and services across systems. On a successful exploitation, the attacker can read and modify some sensitive information but can also be used to lock up any element or operation of the system making that it unresponsive or unavailable.	2023-03-14T05:15:29.227	2023-03-14T13:33:10.470
CVE-2023-25616	9.9	'In some scenario, SAP Business Objects Business Intelligence Platform (CMC) - versions 420, 430, Program Object execution can lead to code injection vulnerability which could allow an attacker to gain access to resources that are allowed by extra privileges. Successful attack could highly impact the confidentiality, Integrity, and Availability of the system.	2023-03-14T05:15:29.773	2023-03-14T13:33:10.470
CVE-2023-25617	9.0	'SAP Business Object (Adaptive Job Server) - versions 420, 430, allows remote execution of arbitrary commands on Unix, when program objects execution is enabled, to authenticated users with scheduling rights, using the BI Launchpad, Central Management Console or a custom application based on the public java SDK. Programs could impact the confidentiality, integrity and availability of the system.	2023-03-14T05:15:29.877	2023-03-14T13:33:10.470

CVE-2023-27269	9.6	'SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an available service to overwrite the system files. In this attack, no data can be read but potentially critical OS files can be overwritten making the system unavailable.	2023-03-14T05:15:30.507	2023-03-14T13:33:10.470
CVE-2023-27500	9.6	'An attacker with non-administrative authorizations can exploit a directory traversal flaw in program SAPRSBRO to over-write system files. In this attack, no data can be read but potentially critical OS files can be over-written making the system unavailable.	2023-03-14T06:15:12.100	2023-03-14T13:33:10.470
CVE-2023-25957	9.1	'A vulnerability has been identified in Mendix SAML (Mendix 7 compatible) (All Versions >= 1.16.4 < 1.17.2), Mendix SAML (Mendix 8 compatible) (All versions >= 2.2.0 < 2.2.3), Mendix SAML (Mendix 9 compatible, New Track) (All versions >= 3.1.9 < 3.2.5), Mendix SAML (Mendix 9 compatible, Upgrade Track) (All versions >= 3.1.9 < 3.2.5). The affected versions of the module insufficiently verifies the SAML assertions. This could allow unauthenticated remote attackers to bypass authentication and get access to the application.	2023-03-14T10:15:28.577	2023-03-14T13:33:10.470
CVE-2022-39214	9.6	"Combodo iTop is an open source, web-based IT service management platform. Prior to versions 2.7.8 and 3.0.2-1, a user who can log in on iTop is able to take over any account just by knowing the account's username. This issue is fixed in versions 2.7.8 and 3.0.2-1."	2023-03-14T16:15:10.277	2023-03-14T16:55:24.767
CVE-2023-21708	9.8	'Remote Procedure Call Runtime Remote Code Execution Vulnerability	2023-03-14T17:15:11.933	2023-03-14T18:04:16.093
CVE-2023-23392	9.8	'HTTP Protocol Stack Remote Code Execution Vulnerability	2023-03-14T17:15:12.793	2023-03-14T18:04:16.093
CVE-2023-23397	9.8	'Microsoft Outlook Elevation of Privilege Vulnerability	2023-03-14T17:15:13.263	2023-03-14T18:04:16.093
CVE-2023-23415	9.8	'Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability	2023-03-14T17:15:14.857	2023-03-14T18:04:09.710

Vulnerabilidades de Severidade Alta

ID	CVSS Score	Descrição	Publicado em	Última modificação

CVE-2023-27088	8.8	'feiqu-opensource Background Vertical authorization vulnerability exists in IndexController.java. demo users with low permission can perform operations within the permission of the admin super administrator and can use this vulnerability to change the blacklist IP address in the system at will.	2023-03-08T16:15:09.527	2023-03-14T15:29:45.970
CVE-2022-46394	8.8	'An issue was discovered in the Arm Mali GPU Kernel Driver. A non-privileged user can make improper GPU processing operations to gain access to already freed memory. This affects Valhall r39p0 through r41p0 before r42p0, and Avalon r41p0 before r42p0.	2023-03-08T19:15:10.613	2023-03-14T15:17:00.400
CVE-2023-1276	4.7	'A vulnerability, which was classified as critical, has been found in SULISS_shop. This issue affects some unknown processing of the file application\\merch\\controller\\Order.php. The manipulation of the argument keyword leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-222599.	2023-03-08T19:15:10.677	2023-03-14T15:15:05.453
CVE-2023-1277	7.8	'A vulnerability, which was classified as critical, was found in kylin-system-updater up to 1.4.20kord. Affected is the function InstallSnap of the component Update Handler. The manipulation leads to command injection. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222600.	2023-03-08T19:15:10.760	2023-03-14T19:29:08.297
CVE-2023-23760	8.8	'A path traversal vulnerability was identified in GitHub Enterprise Server that allowed remote code execution when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to versions 3.8 and was fixed in versions 3.7.7, 3.6.10, 3.5.14, and 3.4.17. This vulnerability was reported via the GitHub Bug Bounty program.	2023-03-08T19:15:10.933	2023-03-14T20:58:50.660
CVE-2023-27486	8.8	'xCAT is a toolkit for deployment and administration of computer clusters. In versions prior to 2.16.5 if zones are configured as a mechanism to secure clusters in XCAT, it is possible for a local root user from one node to obtain credentials to SSH to any node in any zone, except the management node of the default zone. XCAT zones are not enabled by default. Only users that use the optional zone feature are impacted. All versions of xCAT prior to xCAT 2.16.5 are vulnerable. This problem has been fixed in xCAT 2.16.5. Users making use of zones should upgrade to 2.16.5. Users unable to upgrade may mitigate the issue by disabling zones or patching the management node with the fix contained in commit `85149c37f49`.	2023-03-08T19:15:11.073	2023-03-15T14:12:48.077

CVE-2023-22890	7.5	'SmartBear Zephyr Enterprise through 7.15.0 allows unauthenticated users to upload large files, which could exhaust the local drive space, causing a denial of service condition.	2023-03-08T21:15:10.703	2023-03-14T21:00:11.847
CVE-2023-22892	7.5	'There exists an information disclosure vulnerability in SmartBear Zephyr Enterprise through 7.15.0 that could be exploited by unauthenticated users to read arbitrary files from Zephyr instances.	2023-03-08T21:15:10.820	2023-03-14T20:20:47.043
CVE-2023-0030	7.8	'A use-after-free flaw was found in the Linux kernel's nouveau driver in how a user triggers a memory overflow that causes the nvkm_vma_tail function to fail. This flaw allows a local user to crash or potentially escalate their privileges on the system.	2023-03-08T23:15:10.963	2023-03-14T19:48:10.110
CVE-2023-26948	7.5	'onekeyadmin v1.3.9 was discovered to contain an arbitrary file read vulnerability via the component /admin1/file/download.	2023-03-09T01:15:10.383	2023-03-15T14:02:37.153
CVE-2023-26109	7.3	'All versions of the package node-bluetooth-serial-port are vulnerable to Buffer Overflow via the findSerialPortChannel method due to improper user input length validation.	2023-03-09T05:15:56.490	2023-03-09T14:01:48.500
CVE-2023-26110	7.3	'All versions of the package node-bluetooth are vulnerable to Buffer Overflow via the findSerialPortChannel method due to improper user input length validation.	2023-03-09T05:15:56.947	2023-03-09T14:01:48.500
CVE-2023-25573	8.6	'metersphere is an open source continuous testing platform. In affected versions an improper access control vulnerability exists in `/api/jmeter/download/files`, which allows any user to download any file without authentication. This issue may expose all files available to the running process. This issue has been addressed in version 1.20.20 lts and 2.7.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-03-09T17:15:10.600	2023-03-09T20:03:55.143
CVE-2023-25814	7.1	'metersphere is an open source continuous testing platform. In versions prior to 2.7.1 a user who has permission to create a resource file through UI operations is able to append a path to their submission query which will be read by the system and displayed to the user. This allows a users of the system to read arbitrary files on the filesystem of the server so long as the server process itself has permission to read the requested files. This issue has been addressed in version 2.7.1. All users are advised to upgrade. There are no known workarounds for this issue.	2023-03-09T18:15:09.343	2023-03-09T20:03:55.143

CVE-2023-27490	8.1	"NextAuth.js is an open source authentication solution for Next.js applications. `next-auth` applications using OAuth provider versions before `v4.20.1` have been found to be subject to an authentication vulnerability. A bad actor who can read traffic on the victim's network or who is able to social engineer the victim to click a manipulated login link could intercept and tamper with the authorization URL to **log in as the victim**, bypassing the CSRF protection. This is due to a partial failure during a compromised OAuth session where a session code is erroneously generated. This issue has been addressed in version 4.20.1. Users are advised to upgrade. Users unable to upgrade may using Advanced Initialization, manually check the callback request for state, pkce, and nonce against the provider configuration to prevent this issue. See the linked GHSA for details."	2023-03-09T21:15:11.913	2023-03-10T13:53:24.757
CVE-2023-0050	8.7	'An issue has been discovered in GitLab affecting all versions starting from 13.7 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. A specially crafted Kroki diagram could lead to a stored XSS on the client side which allows attackers to perform arbitrary actions on behalf of victims.	2023-03-09T22:15:51.523	2023-03-10T13:53:24.757
CVE-2023-0621	7.8	'Cscape Envision RV version 4.60 is vulnerable to an out-of-bounds read vulnerability when parsing project (i.e. HMI) files. The product lacks proper validation of user-supplied data, which could result in reads past the end of allocated data structures. An attacker could leverage these vulnerabilities to execute arbitrary code in the context of the current process.	2023-03-09T22:15:51.597	2023-03-13T03:50:19.833
CVE-2023-0622	7.8	'Cscape Envision RV version 4.60 is vulnerable to an out-of-bounds write vulnerability when parsing project (i.e. HMI) files. The product lacks proper validation of user-supplied data, which could result in writes past the end of allocated data structures. An attacker could leverage these vulnerabilities to execute arbitrary code in the context of the current process.	2023-03-09T22:15:51.667	2023-03-13T03:50:29.020
CVE-2023-0623	7.8	'Cscape Envision RV version 4.60 is vulnerable to an out-of-bounds write vulnerability when parsing project (i.e. HMI) files. The product lacks proper validation of user-supplied data, which could result in writes past the end of allocated data structures. An attacker could leverage these vulnerabilities to execute arbitrary code in the context of the current process.	2023-03-09T22:15:51.737	2023-03-13T03:50:35.700

CVE-2023-20049	8.6	'A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads.	2023-03-09T22:15:52.200	2023-03-10T13:53:24.757
CVE-2022-3767	7.7	'Missing validation in DAST analyzer affecting all versions from 1.11.0 prior to 3.0.32, allows custom request headers to be sent with every request, regardless of the host.	2023-03-09T23:15:10.833	2023-03-10T13:53:24.757
CVE-2023-22301	7.5	'The kernel subsystem hmdfs within OpenHarmony-v3.1.5 and prior versions has an arbitrary memory accessing vulnerability which network attackers can launch a remote attack to obtain kernel memory data of the target system.	2023-03-10T11:15:12.127	2023-03-14T18:00:19.000
CVE-2023-22436	7.8	'The kernel subsystem function check_permission_for_set_tokenid within OpenHarmony-v3.1.5 and prior versions has an UAF vulnerability which local attackers can exploit this vulnerability to escalate the privilege to root.	2023-03-10T11:15:12.220	2023-03-14T17:59:28.937
CVE-2023-1313	7.2	'Unrestricted Upload of File with Dangerous Type in GitHub repository cockpit-hq/cockpit prior to 2.4.1.	2023-03-10T12:15:21.633	2023-03-10T13:53:17.070
CVE-2023-1320	7.1	'Cross-site Scripting (XSS) - Stored in GitHub repository osticket/osticket prior to v1.16.6.	2023-03-10T16:15:11.010	2023-03-13T03:47:55.653
CVE-2023-26075	7.6	'An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, Exynos Auto T5123, and Exynos W920. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List.	2023-03-10T17:15:10.160	2023-03-10T17:23:46.767
CVE-2021-27788	8.3	"HCL Verse is susceptible to a Cross Site Scripting (XSS) vulnerability. By tricking a user into clicking a crafted URL, a remote unauthenticated attacker could execute script in a victim's web browser to perform operations as the victim and/or steal the victim's cookies, session tokens, or other sensitive information."	2023-03-10T21:15:10.867	2023-03-11T02:54:29.333

CVE-2022-20929	7.8	'A vulnerability in the upgrade signature verification of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an unauthenticated, local attacker to provide an unauthentic upgrade file for upload. This vulnerability is due to insufficient cryptographic signature verification of upgrade files. An attacker could exploit this vulnerability by providing an administrator with an unauthentic upgrade file. A successful exploit could allow the attacker to fully compromise the Cisco NFVIS system.	2023-03-10T21:15:10.963	2023-03-11T02:54:29.333
CVE-2022-25655	8.4	'Memory corruption in WLAN HAL while arbitrary value is passed in WMI UTF command payload.	2023-03-10T21:15:11.117	2023-03-11T02:54:29.333
CVE-2022-25694	8.4	'Memory corruption in Modem due to usage of Out-of-range pointer offset in UIM	2023-03-10T21:15:11.190	2023-03-11T02:54:29.333
CVE-2022-25705	7.8	'Memory corruption in modem due to integer overflow to buffer overflow while handling APDU response	2023-03-10T21:15:11.257	2023-03-11T02:54:29.333
CVE-2022-25709	8.4	'Memory corruption in modem due to use of out of range pointer offset while processing qmi msg	2023-03-10T21:15:11.340	2023-03-11T02:54:29.333
CVE-2022-33213	7.5	'Memory corruption in modem due to buffer overflow while processing a PPP packet	2023-03-10T21:15:11.487	2023-03-11T02:54:29.333
CVE-2022-33242	7.8	'Memory corruption due to improper authentication in Qualcomm IPC while loading unsigned lib in audio PD.	2023-03-10T21:15:11.557	2023-03-11T02:54:29.333
CVE-2022-33244	7.5	'Transient DOS due to reachable assertion in modem during MIB reception and SIB timeout	2023-03-10T21:15:11.620	2023-03-11T02:54:29.333
CVE-2022-33250	7.5	'Transient DOS due to reachable assertion in modem when network repeatedly sent invalid message container for NR to LTE handover.	2023-03-10T21:15:11.757	2023-03-11T02:54:29.333
CVE-2022-33254	7.5	'Transient DOS due to reachable assertion in Modem while processing SIB1 Message.	2023-03-10T21:15:11.830	2023-03-11T02:54:29.333
CVE-2022-33272	7.5	'Transient DOS in modem due to reachable assertion.	2023-03-10T21:15:12.100	2023-03-11T02:54:29.333
CVE-2022-33278	7.8	'Memory corruption due to buffer copy without checking the size of input in HLOS when input message size is larger than the buffer capacity.	2023-03-10T21:15:12.167	2023-03-11T02:54:29.333
CVE-2022-33309	7.5	'Transient DOS due to buffer over-read in WLAN Firmware while parsing secure FTMR frame with size lesser than 39 Bytes.	2023-03-10T21:15:12.233	2023-03-11T02:54:29.333
CVE-2022-40515	7.3	'Memory corruption in Video due to double free while playing 3gp clip with invalid metadata atoms.	2023-03-10T21:15:12.380	2023-03-11T02:54:29.333

CVE-2022-40527	7.5	'Transient DOS due to reachable assertion in WLAN while processing PEER ID populated by TQM.	2023-03-10T21:15:12.453	2023-03-11T02:54:29.333
CVE-2022-40530	8.4	'Memory corruption in WLAN due to integer overflow to buffer overflow in WLAN during initialization phase.	2023-03-10T21:15:12.523	2023-03-11T02:54:29.333
CVE-2022-40531	8.4	'Memory corruption in WLAN due to incorrect type cast while sending WMI_SCAN_SCH_PRIO_TBL_CMDID message.	2023-03-10T21:15:12.597	2023-03-11T02:54:29.333
CVE-2022-40535	7.5	'Transient DOS due to buffer over-read in WLAN while sending a packet to device.	2023-03-10T21:15:12.673	2023-03-11T02:54:29.333
CVE-2022-40537	7.3	'Memory corruption in Bluetooth HOST while processing the AVRC_PDU_GET_PLAYER_APP_VALUE_TEXT AVRCP response.	2023-03-10T21:15:12.753	2023-03-11T02:54:29.333
CVE-2022-40539	8.4	'Memory corruption in Automotive Android OS due to improper validation of array index.	2023-03-10T21:15:12.820	2023-03-11T02:54:29.333
CVE-2022-40540	8.4	'Memory corruption due to buffer copy without checking the size of input while loading firmware in Linux Kernel.	2023-03-10T21:15:12.887	2023-03-11T02:54:29.333
CVE-2023-1355	8.4	'NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.1402.	2023-03-11T22:15:10.133	2023-03-13T11:25:01.697
CVE-2023-1357	7.3	"A vulnerability, which was classified as critical, has been found in SourceCodester Simple Bakery Shop Management System 1.0. Affected by this issue is some unknown functionality of the component Admin Login. The manipulation of the argument username/password with the input admin' or 1=1 -- leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222860."	2023-03-12T08:15:09.597	2023-03-13T11:25:01.697
CVE-2023-1361	7.2	'SQL Injection in GitHub repository unilogies/bumsys prior to v2.0.2.	2023-03-13T05:15:11.827	2023-03-13T11:25:01.697
CVE-2023-1362	8.4	'Improper Restriction of Rendered UI Layers or Frames in GitHub repository unilogies/bumsys prior to v2.0.2.	2023-03-13T05:15:11.933	2023-03-13T11:25:01.697

CVE-2023-1365	7.3	'A vulnerability was found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/ajax.php. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222872.	2023-03-13T08:15:10.140	2023-03-13T11:25:01.697
CVE-2023-1368	7.3	'A vulnerability was found in XHCMS 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php of the component POST Parameter Handler. The manipulation of the argument user leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-222874 is the identifier assigned to this vulnerability.	2023-03-13T09:15:10.807	2023-03-13T11:25:01.697
CVE-2023-0629	7.1	"Docker Desktop before 4.17.0 allows an unprivileged user to bypass Enhanced Container Isolation (ECI) restrictions by setting the Docker host to docker.raw.sock, or npipe:////.pipe/docker_engine_linux on Windows, via the -H (--host) CLI flag or the DOCKER_HOST environment variable and launch containers without the additional hardening features provided by ECI. This would not affect already running containers, nor containers launched through the usual approach (without Docker's raw socket). The affected functionality is available for Docker Business customers only and assumes an environment where users are not granted local root or Administrator privileges. This issue has been fixed in Docker Desktop 4.17.0. Affected Docker Desktop versions: from 4.13.0 before 4.17.0."	2023-03-13T12:15:11.060	2023-03-13T12:21:25.843
CVE-2023-24033	7.5	'The Samsung Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets do not properly check format types specified by the Session Description Protocol (SDP) module, which can lead to a denial of service.	2023-03-13T12:15:11.160	2023-03-13T12:21:25.843
CVE-2023-26072	7.6	'An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, Exynos Auto T5123, and Exynos W920. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list.	2023-03-13T12:15:11.307	2023-03-13T12:21:25.843
CVE-2023-1372	7.2	'The WH Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several parameters such as wh_homepage, wh_text_short, wh_text_full and in versions up to, and including, 3.0.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-03-13T13:15:11.503	2023-03-13T14:48:34.443

CVE-2023-26074	7.6	'An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, Exynos Auto T5123, and Exynos W920. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions.	2023-03-13T13:15:11.903	2023-03-13T14:48:34.443
CVE-2022-31474	7.5	'Directory Traversal vulnerability in iThemes BackupBuddy plugin 8.5.8.0 - 8.7.4.1 versions.	2023-03-13T14:15:12.507	2023-03-13T14:48:34.443
CVE-2023-26073	7.6	'An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, Exynos Auto T5123, and Exynos W920. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list.	2023-03-13T14:15:12.973	2023-03-13T14:48:34.443
CVE-2023-26076	7.6	'An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G SM message codec can occur due to insufficient parameter validation when decoding reserved options.	2023-03-13T15:15:12.720	2023-03-13T15:23:59.393
CVE-2023-27580	7.5	"CodeIgniter Shield provides authentication and authorization for the CodeIgniter 4 PHP framework. An improper implementation was found in the password storage process. All hashed passwords stored in Shield v1.0.0-beta.3 or earlier are easier to crack than expected due to the vulnerability. Therefore, they should be removed as soon as possible. If an attacker gets (1) the user's hashed password by Shield, and (2) the hashed password (SHA-384 hash without salt) from somewhere, the attacker may easily crack the user's password. Upgrade to Shield v1.0.0-beta.4 or later to fix this issue. After upgrading, all users' hashed passwords should be updated (saved to the database). There are no known workarounds."	2023-03-13T18:15:12.970	2023-03-13T18:19:41.787
CVE-2023-25802	7.5	"Roxy-WI is a Web interface for managing Haproxy, Nginx, Apache, and Keepalived servers. Versions prior to 6.3.6.0 don't correctly neutralize `dir/../filename` sequences, such as `/etc/nginx/../passwd`, allowing an actor to gain information about a server. Version 6.3.6.0 has a patch for this issue."	2023-03-13T20:15:14.967	2023-03-14T13:33:10.470
CVE-2023-25803	7.5	'Roxy-WI is a Web interface for managing Haproxy, Nginx, Apache, and Keepalived servers. Versions prior to 6.3.5.0 have a directory traversal vulnerability allows the inclusion of server-side files. This issue is fixed in version 6.3.5.0.	2023-03-13T20:15:15.057	2023-03-14T13:33:10.470

CVE-2023-0346	7.5	'Akuvox E11 cloud login is performed through an unencrypted HTTP connection. An attacker could gain access to the Akuvox cloud and device if the MAC address of a device if known.	2023-03-13T21:15:13.137	2023-03-14T13:33:10.470
CVE-2023-0347	7.5	'The Akuvox E11 Media Access Control (MAC) address, a primary identifier, combined with the Akuvox E11 IP address, could allow an attacker to identify the device on the Akuvox cloud.	2023-03-13T21:15:13.220	2023-03-14T13:33:10.470
CVE-2023-0348	7.5	'Akuvox E11 allows direct SIP calls. No access control is enforced by the SIP servers, which could allow an attacker to contact any device within Akuvox to call any other device.	2023-03-13T21:15:13.303	2023-03-14T13:33:10.470
CVE-2023-0349	7.5	'The Akuvox E11 libvoice library provides unauthenticated access to the camera capture for image and video. This could allow an attacker to view and record image and video from the camera.	2023-03-13T21:15:13.393	2023-03-14T13:33:10.470
CVE-2023-0351	8.8	'The Akuvox E11 web server backend library allows command injection in the device phone-book contacts functionality. This could allow an attacker to upload files with executable command instructions.	2023-03-13T21:15:13.563	2023-03-14T13:33:10.470
CVE-2023-0353	7.2	'Akuvox E11 uses a weak encryption algorithm for stored passwords and uses a hard-coded password for decryption which could allow the encrypted passwords to be decrypted from the configuration file.	2023-03-13T21:15:13.807	2023-03-14T13:33:10.470
CVE-2023-27581	8.8	"github-slug-action is a GitHub Action to expose slug value of GitHub environment variables inside of one's GitHub workflow. Starting in version 4.0.0` and prior to version 4.4.1, this action uses the `github.head_ref` parameter in an insecure way. This vulnerability can be triggered by any user on GitHub on any workflow using the action on pull requests. They just need to create a pull request with a branch name, which can contain the attack payload. This can be used to execute code on the GitHub runners and to exfiltrate any secrets one uses in the CI pipeline. A patched action is available in version 4.4.1. No workaround is available."	2023-03-13T21:15:14.037	2023-03-14T13:33:10.470
CVE-2023-27587	7.4	'ReadtoMyShoe, a web app that lets users upload articles and listen to them later, generates an error message containing sensitive information prior to commit 8533b01. If an error occurs when adding an article, the website shows the user an error message. If the error originates from the Google Cloud TTS request, then it will include the full URL of the request. The request URL contains the Google Cloud API key. This has been patched in commit 8533b01. Upgrading should be accompanied by deleting the current GCP API key and issuing a new one. There are no known workarounds.	2023-03-13T22:15:12.483	2023-03-14T21:15:10.670

CVE-2023-26459	7.4	'Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, an attacker authenticated as a non-administrative user can craft a request which will trigger the application server to send a request to an arbitrary URL which can reveal, modify or make unavailable non-sensitive information, leading to low impact on Confidentiality, Integrity and Availability.	2023-03-14T05:15:30.160	2023-03-14T13:33:10.470
CVE-2023-27498	7.2	'SAP Host Agent (SAPOSCOL) - version 7.22, allows an unauthenticated attacker with network access to a server port assigned to the SAP Start Service to submit a crafted request which results in a memory corruption error. This error can be used to reveal but not modify any technical information about the server. It can also make a particular service temporarily unavailable	2023-03-14T06:15:11.973	2023-03-14T13:33:10.470
CVE-2023-27501	8.7	'SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient validation of path information provided by users, thus exploiting a directory traversal flaw in an available service to delete system files. In this attack, no data can be read but potentially critical OS files can be deleted making the system unavailable, causing significant impact on both availability and integrity	2023-03-14T06:15:12.213	2023-03-14T13:33:10.470
CVE-2023-27893	8.8	'An attacker authenticated as a user with a non-administrative role and a common remote execution authorization in SAP Solution Manager and ABAP managed systems (ST-PI) - versions 2088_1_700, 2008_1_710, 740, can use a vulnerable interface to execute an application function to perform actions which they would not normally be permitted to perform. Depending on the function executed, the attack can read or modify any user or application data and can make the application unavailable.	2023-03-14T06:15:12.333	2023-03-14T13:33:10.470
CVE-2023-27398	7.8	'A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20304)	2023-03-14T10:15:28.873	2023-03-14T13:33:10.470
CVE-2023-27399	7.8	'A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20299, ZDI-CAN-20346)	2023-03-14T10:15:28.963	2023-03-14T13:33:10.470

CVE-2023-27400	7.8	'A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20300)	2023-03-14T10:15:29.050	2023-03-14T13:33:10.470
CVE-2023-27401	7.8	'A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20308, ZDI-CAN-20345)	2023-03-14T10:15:29.143	2023-03-14T13:33:10.470
CVE-2023-27402	7.8	'A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20334)	2023-03-14T10:15:29.240	2023-03-14T13:33:10.470
CVE-2023-27403	7.8	'A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains a memory corruption vulnerability while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20303, ZDI-CAN-20348)	2023-03-14T10:15:29.337	2023-03-14T13:33:10.470
CVE-2023-27404	7.8	'A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application is vulnerable to stack-based buffer while parsing specially crafted SPP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-20433)	2023-03-14T10:15:29.427	2023-03-14T13:33:10.470
CVE-2023-27405	7.8	'A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20432)	2023-03-14T10:15:29.513	2023-03-14T13:33:10.470
CVE-2023-27406	7.8	'A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application is vulnerable to stack-based buffer while parsing specially crafted SPP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-20449)	2023-03-14T10:15:29.597	2023-03-14T13:33:10.470
CVE-2023-27463	8.8	'A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.3). The audit log form of affected applications is vulnerable to SQL injection. This could allow authenticated remote attackers to execute arbitrary SQL queries on the server database.	2023-03-14T10:15:29.757	2023-03-14T13:33:10.470
CVE-2023-1299	7.4	'HashiCorp Nomad and Nomad Enterprise 1.5.0 allow a job submitter to escalate to management-level privileges using workload identity and task API. Fixed in 1.5.1.	2023-03-14T15:15:11.593	2023-03-14T16:55:24.767

CVE-2022-39216	7.4	'Combodo iTop is an open source, web-based IT service management platform. Prior to versions 2.7.8 and 3.0.2-1, the reset password token is generated without any randomness parameter. This may lead to account takeover. The issue is fixed in versions 2.7.8 and 3.0.2-1.	2023-03-14T16:15:10.377	2023-03-14T16:55:24.767
CVE-2023-23383	8.2	'Service Fabric Explorer Spoofing Vulnerability	2023-03-14T17:15:12.317	2023-03-14T18:04:16.093
CVE-2023-23385	7.0	'Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability	2023-03-14T17:15:12.440	2023-03-14T18:04:16.093
CVE-2023-23388	8.8	'Windows Bluetooth Driver Elevation of Privilege Vulnerability	2023-03-14T17:15:12.530	2023-03-14T18:04:16.093
CVE-2023-23393	7.0	'Windows BrokerInfrastructure Service Elevation of Privilege Vulnerability	2023-03-14T17:15:12.883	2023-03-14T18:04:16.093
CVE-2023-23398	7.1	'Microsoft Excel Spoofing Vulnerability	2023-03-14T17:15:13.350	2023-03-14T18:04:16.093
CVE-2023-23399	7.8	'Microsoft Excel Remote Code Execution Vulnerability	2023-03-14T17:15:13.430	2023-03-14T18:04:16.093
CVE-2023-23400	7.2	'Windows DNS Server Remote Code Execution Vulnerability	2023-03-14T17:15:13.517	2023-03-14T18:04:16.093
CVE-2023-23401	7.8	'Windows Media Remote Code Execution Vulnerability	2023-03-14T17:15:13.610	2023-03-14T18:04:16.093
CVE-2023-23402	7.8	'Windows Media Remote Code Execution Vulnerability	2023-03-14T17:15:13.700	2023-03-14T18:04:09.710
CVE-2023-23403	8.8	'Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	2023-03-14T17:15:13.787	2023-03-14T18:04:09.710
CVE-2023-23404	8.1	'Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability	2023-03-14T17:15:13.870	2023-03-14T18:04:09.710
CVE-2023-23405	8.1	'Remote Procedure Call Runtime Remote Code Execution Vulnerability	2023-03-14T17:15:13.963	2023-03-14T18:04:09.710
CVE-2023-23406	8.8	'Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	2023-03-14T17:15:14.050	2023-03-14T18:04:09.710
CVE-2023-23407	7.1	'Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability	2023-03-14T17:15:14.130	2023-03-14T18:04:09.710

CVE-2023-23410	7.8	'Windows HTTP.sys Elevation of Privilege Vulnerability	2023-03-14T17:15:14.407	2023-03-14T18:04:09.710
CVE-2023-23412	7.8	'Windows Accounts Picture Elevation of Privilege Vulnerability	2023-03-14T17:15:14.593	2023-03-14T18:04:09.710
CVE-2023-23413	8.8	'Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	2023-03-14T17:15:14.680	2023-03-14T18:04:09.710
CVE-2023-23414	7.1	'Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability	2023-03-14T17:15:14.767	2023-03-14T18:04:09.710
CVE-2023-23416	8.4	'Windows Cryptographic Services Remote Code Execution Vulnerability	2023-03-14T17:15:14.967	2023-03-14T18:04:09.710
CVE-2023-23417	7.8	'Windows Partition Management Driver Elevation of Privilege Vulnerability	2023-03-14T17:15:15.110	2023-03-14T18:04:09.710
CVE-2023-23418	7.8	'Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability	2023-03-14T17:15:15.260	2023-03-14T18:04:09.710
CVE-2023-23419	7.8	'Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability	2023-03-14T17:15:15.370	2023-03-14T18:04:09.710
CVE-2023-23420	7.8	'Windows Kernel Elevation of Privilege Vulnerability	2023-03-14T17:15:15.470	2023-03-14T18:04:09.710
CVE-2023-23421	7.8	'Windows Kernel Elevation of Privilege Vulnerability	2023-03-14T17:15:15.563	2023-03-14T18:04:09.710
CVE-2023-23422	7.8	'Windows Kernel Elevation of Privilege Vulnerability	2023-03-14T17:15:15.657	2023-03-14T18:04:03.023
CVE-2023-23423	7.8	'Windows Kernel Elevation of Privilege Vulnerability	2023-03-14T17:15:15.747	2023-03-14T18:04:03.023
CVE-2023-24859	7.5	'Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability	2023-03-14T17:15:16.123	2023-03-14T18:04:03.023
CVE-2023-24861	7.0	'Windows Graphics Component Elevation of Privilege Vulnerability	2023-03-14T17:15:16.223	2023-03-14T18:04:03.023
CVE-2023-24864	8.8	'Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability	2023-03-14T17:15:16.520	2023-03-14T18:04:03.023

CVE-2023-24867	8.8	'Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	2023-03-14T17:15:16.807	2023-03-14T18:04:03.023
CVE-2023-24868	8.8	'Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	2023-03-14T17:15:16.900	2023-03-14T18:04:03.023
CVE-2023-24869	8.1	'Remote Procedure Call Runtime Remote Code Execution Vulnerability	2023-03-14T17:15:17.007	2023-03-14T18:04:03.023
CVE-2023-24871	8.8	'Windows Bluetooth Service Remote Code Execution Vulnerability	2023-03-14T17:15:17.223	2023-03-14T18:04:03.023
CVE-2023-24872	8.8	'Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	2023-03-14T17:15:17.337	2023-03-14T18:04:03.023
CVE-2023-24876	8.8	'Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	2023-03-14T17:15:17.453	2023-03-14T18:04:03.023
CVE-2023-24892	7.1	'Microsoft Edge (Chromium-based) Webview2 Spoofing Vulnerability	2023-03-14T17:15:18.197	2023-03-14T18:03:58.047
CVE-2023-24907	8.8	'Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	2023-03-14T17:15:18.400	2023-03-14T18:03:58.047
CVE-2023-24908	8.1	'Remote Procedure Call Runtime Remote Code Execution Vulnerability	2023-03-14T17:15:18.490	2023-03-14T18:03:58.047
CVE-2023-24909	8.8	'Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	2023-03-14T17:15:18.577	2023-03-14T18:03:58.047
CVE-2023-24910	7.8	'Windows Graphics Component Elevation of Privilege Vulnerability	2023-03-14T17:15:18.670	2023-03-14T18:03:58.047
CVE-2023-24913	8.8	'Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	2023-03-14T17:15:18.850	2023-03-14T18:03:58.047
CVE-2023-24930	7.8	'Microsoft OneDrive for MacOS Elevation of Privilege Vulnerability	2023-03-14T17:15:19.427	2023-03-14T18:03:58.047

CVE-2023-27585	7.5	"PJSIP is a free and open source multimedia communication library written in C. A buffer overflow vulnerability in versions 2.13 and prior affects applications that use PJSIP DNS resolver. It doesn't affect PJSIP users who do not utilise PJSIP DNS resolver. This vulnerability is related to CVE-2022-24793. A patch is available as commit `d1c5e4d` in the `master` branch. A workaround is to disable DNS resolution in PJSIP config (by setting `nameserver_count` to zero) or use an external resolver implementation instead."	2023-03-14T17:15:19.587	2023-03-14T18:03:58.047
CVE-2023-27588	7.5	'Hasura is an open-source product that provides users GraphQL or REST APIs. A path traversal vulnerability has been discovered within Hasura GraphQL Engine prior to versions 1.3.4, 2.55.1, 2.20.1, and 2.21.0-beta1. Projects running on Hasura Cloud were not vulnerable. Self-hosted Hasura Projects with deployments that are publicly exposed and not protected by a WAF or other HTTP protection layer should be upgraded to version 1.3.4, 2.55.1, 2.20.1, or 2.21.0-beta1 to receive a patch.	2023-03-14T18:15:10.460	2023-03-15T12:42:25.297
CVE-2023-27590	7.8	'Rizin is a UNIX-like reverse engineering framework and command-line toolset. In version 0.5.1 and prior, converting a GDB registers profile file into a Rizin register profile can result in a stack-based buffer overflow when the `name`, `type`, or `groups` fields have longer values than expected. Users opening untrusted GDB registers files (e.g. with the `drpg` or `arpg` commands) are affected by this flaw. Commit d6196703d89c84467b600ba2692534579dc25ed4 contains a patch for this issue. As a workaround, review the GDB register profiles before loading them with `drpg`/`arpg` commands.	2023-03-14T21:15:10.763	2023-03-15T12:42:18.907