IBLISS DIGITAL SECURITY

Vulnerabilidades Publicadas Na Semana

Vulnerabilidades de Severidade Crítica

ID	CVSS Score	Descrição	Publicado em	Última Modificação
CVE-2023-24726	9.8	Art Gallery Management System v1.0 was discovered to contain a SQL injection vulnerability via the viewid parameter on the enquiry page.	2023-03-15T14:15:11.563	2023-03-17T18:19:15.197
CVE-2023-1379	6.3	A vulnerability was found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. It has been rated as critical. This issue affects some unknown processing of the file addmem.php of the component POST Parameter Handler. The manipulation of the argument firstname leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223127.	2023-03-15T16:15:10.883	2023-03-20T20:35:17.667
CVE-2023-1416	6.3	A vulnerability classified as critical has been found in Simple Art Gallery 1.0. Affected is an unknown function of the file adminHome.php. The manipulation of the argument social_facebook leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223128.	2023-03-15T16:15:11.060	2023-03-20T20:37:07.557
CVE-2020-27507	9.8	The Kamailio SIP before 5.5.0 server mishandles INVITE requests with duplicated fields and overlength tag, leading to a buffer overflow that crashes the server or possibly have unspecified other impact.	2023-03-15T20:15:10.283	2023-03-19T03:50:16.077
CVE-2023-25344	9.8	An issue was discovered in swig-templates thru 2.0.4 and swig thru 1.4.2, allows attackers to execute arbitrary code via crafted Object.prototype anonymous function.	2023-03-15T20:15:10.480	2023-03-18T03:50:33.213
CVE-2023-24468	9.8	Broken access control in Advanced Authentication versions prior to 6.4.1.1 and 6.3.7.2	2023-03-15T23:15:09.563	2023-03-19T03:47:27.013

CVE-2023-25280	9.8	OS Command injection vulnerability in D-Link DIR820LA1_FW105B03 allows attackers to escalate privileges to root via a crafted payload with the ping_addr parameter to ping.ccp.	2023-03-16T01:15:46.780	2023-03-21T17:33:33.767
CVE-2023-1432	7.3	A vulnerability was found in SourceCodester Online Food Ordering System 2.0 and classified as critical. Affected by this issue is some unknown functionality of the file /fos/admin/ajax.php?action=save_settings of the component POST Request Handler. The manipulation leads to improper access controls. The attack may be launched remotely. VDB-223214 is the identifier assigned to this vulnerability.	2023-03-16T13:15:10.327	2023-03-22T02:32:41.300
CVE-2023-27250	9.8	Online Book Store Project v1.0 is vulnerable to SQL Injection via /bookstore/bookPerPub.php.	2023-03-16T13:15:10.493	2023-03-21T22:42:37.387
CVE-2020-19947	9.6	Cross Site Scripting vulnerability found in Markdown Edit allows a remote attacker to execute arbitrary code via the edit parameter of the webpage.	2023-03-16T15:15:09.910	2023-03-22T01:23:04.440
CVE-2023-28100	10.0	"Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. Versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4 contain a vulnerability similar to CVE-2017-5226, but using the `TIOCLINUX` ioctl command instead of `TIOCSTI`. If a Flatpak app is run on a Linux virtual console such as `/dev/tty1`, it can copy text from the virtual console and paste it into the command buffer, from which the command might be run after the Flatpak app has exited. Ordinary graphical terminal emulators like xterm, gnome-terminal and Konsole are unaffected. This vulnerability is specific to the Linux virtual consoles `/dev/tty1`, `/dev/tty2` and so on. A patch is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, dont run Flatpak on a Linux virtual console. Flatpak is primarily designed to be used in a Wayland or X11 graphical environment.	2023-03-16T16:15:12.553	2023-03-16T18:40:56.770
CVE-2023-0811	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program.	2023-03-16T18:15:11.160	2023-03-16T18:40:56.770
CVE-2023-1256	9.8	The listed versions of AVEVA Plant SCADA and AVEVA Telemetry Server are vulnerable to an improper authorization exploit which could allow an unauthenticated user to remotely read data, cause denial of service, and tamper with alarm states.	2023-03-16T19:15:18.227	2023-03-17T04:04:43.147

CVE-2022-43604	10.0	An out-of-bounds write vulnerability exists in the GetAttributeList attribute_count_request functionality of EIP Stack Group OpENer development commit 58ee13c. A specially crafted EtherNet/IP request can lead to an out-of-bounds write, potentially causing the server to crash or allow for remote code execution. An attacker can send a series of EtherNet/IP requests to trigger this vulnerability.	2023-03-16T21:15:11.123	2023-03-17T04:04:43.147
CVE-2022-43605	10.0	An out-of-bounds write vulnerability exists in the SetAttributeList attribute_count_request functionality of EIP Stack Group OpENer development commit 58ee13c. A specially crafted EtherNet/IP request can lead to an out of bounds write, potentially causing the server to crash or allow for remote code execution. An attacker can send a series of EtherNet/IP requests to trigger this vulnerability.	2023-03-16T21:15:11.203	2023-03-17T04:04:43.147
CVE-2023-21456	9.0	Path traversal vulnerability in Galaxy Themes Service prior to SMR Mar-2023 Release 1 allows attacker to access arbitrary file with system uid.	2023-03-16T21:15:12.050	2023-03-17T04:04:43.147
CVE-2023-1152	9.8	"Improper Neutralization of Special Elements used in an SQL Command (SQL Injection) vulnerability in Utarit Information Technologies Persolus allows SQL Injection. This issue affects Persolus: before 2.03.93.	2023-03-17T09:15:12.533	2023-03-17T12:59:25.697
CVE-2023-28115	9.8	Snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. Prior to version 1.4.2, Snappy is vulnerable to PHAR deserialization due to a lack of checking on the protocol before passing it into the `file_exists()` function. If an attacker can upload files of any type to the server he can pass in the phar:// protocol to unserialize the uploaded file and instantiate arbitrary PHP objects. This can lead to remote code execution especially when snappy is used with frameworks with documented POP chains like Laravel/Symfony vulnerable developer code. If a user can control the output file from the `generateFromHtml()` function, it will invoke deserialization. This vulnerability is capable of remote code execution if Snappy is used with frameworks or developer code with vulnerable POP chains. It has been fixed in version 1.4.2.	2023-03-17T22:15:11.437	2023-03-20T02:46:58.537
CVE-2023-28424	9.1	Soko if the code that powers packages.gentoo.org. Prior to version 1.0.2, the two package search handlers, `Search` and `SearchFeed`, implemented in `pkg/app/handler/packages/search.go`, are affected by a SQL injection via the `q` parameter. As a result, unauthenticated attackers can execute arbitrary SQL queries on `https://packages.gentoo.org/`. It was also demonstrated that primitive was enough to gain code execution in the context of the PostgreSQL container. The issue was addressed in commit `4fa6e4b619c0362728955b6ec56eab0e0cbf1e23y` of version 1.0.2 using prepared statements to interpolate user-controlled data in SQL queries.	2023-03-20T13:15:11.973	2023-03-20T14:02:37.427

CVE-2023-27586	9.9	"CairoSVG is an SVG converter based on Cairo, a 2D graphics library. Prior to version 2.7.0, Cairo can send requests to external hosts when processing SVG files. A malicious actor could send a specially crafted SVG file that allows them to perform a server-side request forgery or denial of service. Version 2.7.0 disables CairoSVGs ability to access other files online by default.	2023-03-20T16:15:13.197	2023-03-21T11:51:09.643
CVE-2023-27578	9.1	Galaxy is an open-source platform for data analysis. All supported versions of Galaxy are affected prior to 22.01, 22.05, and 23.0 are affected by an insufficient permission check. Unsupported versions are likely affected as far back as the functionality of Visualizations/Pages exists. Due to this issue, an attacker can modify or delete any Galaxy Visualization or Galaxy Page given they know the encoded ID of it. Additionally, they can copy or import any Galaxy Visualization given they know the encoded ID of it. Patches are available for versions 22.01, 22.05, and 23.0. For the changes to take effect, you must restart all Galaxy server processes. There are no supported workarounds.	2023-03-20T20:15:52.690	2023-03-21T11:51:09.643
CVE-2023-1153	10.0	"Improper Neutralization of Special Elements used in an SQL Command (SQL Injection) vulnerability in Pacsrapor allows SQL Injection, Command Line Execution through SQL Injection.This issue affects Pacsrapor: before 1.22.	2023-03-21T12:15:10.117	2023-03-21T12:19:40.680
CVE-2023-27874	9.9	IBM Aspera Faspex 4.4.2 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote authenticated attacker could exploit this vulnerability to execute arbitrary commands. IBM X-Force ID: 249845.	2023-03-21T15:15:12.633	2023-03-21T17:00:14.450
CVE-2023-27569	9.8	The eo_tags package before 1.3.0 for PrestaShop allows SQL injection via an HTTP User-Agent or Referer header.	2023-03-21T16:15:13.040	2023-03-21T17:00:14.450
CVE-2023-27570	9.8	The eo_tags package before 1.4.19 for PrestaShop allows SQL injection via a crafted _ga cookie.	2023-03-21T16:15:13.113	2023-03-21T17:00:14.450
CVE-2022-37337	9.1	A command execution vulnerability exists in the access control functionality of Netgear Orbi Router RBR750 4.6.8.5. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2023-03-21T18:15:12.097	2023-03-21T20:07:21.987
CVE-2023-27855	9.8	"In affected versions, a path traversal exists when processing a message in Rockwell Automations ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution.	2023-03-22T00:15:12.670	2023-03-22T12:48:04.240

CVE-2023-25589	9.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to create arbitrary users on the platform. A successful exploit allows an attacker to achieve total cluster compromise.	2023-03-22T06:15:09.837	2023-03-22T12:48:04.240

Vulnerabilidades de Severidade Alta

ID	CVSS Score	Descrição	Publicado em	Última modificação
CVE-2022-47427	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Joseph C Dolson My Calendar plugin <= 3.3.24.1 versions.	2023-03-15T11:15:09.287	2023-03-17T18:33:39.697
CVE-2023-25708	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Rextheme WP VR – 360 Panorama and Virtual Tour Builder For WordPress plugin <= 8.2.7 versions.	2023-03-15T11:15:09.393	2023-03-17T18:37:15.680
CVE-2023-25709	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Plainware Locatoraid Store Locator plugin <= 3.9.11 versions.	2023-03-15T11:15:09.473	2023-03-17T18:40:13.067
CVE-2023-25968	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Cozmoslabs, Madalin Ungureanu, Antohe Cristian Client Portal – Private user pages and login plugin <= 1.1.8 versions.	2023-03-15T11:15:09.550	2023-03-17T18:44:07.267
CVE-2023-24728	8.8	Simple Customer Relationship Management System v1.0 as discovered to contain a SQL injection vulnerability via the contact parameter in the user profile update function.	2023-03-15T14:15:11.623	2023-03-17T18:51:07.130
CVE-2023-24729	8.8	Simple Customer Relationship Management System v1.0 as discovered to contain a SQL injection vulnerability via the address parameter in the user profile update function.	2023-03-15T14:15:11.673	2023-03-17T18:52:50.820
CVE-2023-24730	8.8	Simple Customer Relationship Management System v1.0 as discovered to contain a SQL injection vulnerability via the company parameter in the user profile update function.	2023-03-15T14:15:11.727	2023-03-17T19:01:49.883
CVE-2023-24731	8.8	Simple Customer Relationship Management System v1.0 as discovered to contain a SQL injection vulnerability via the query parameter in the user profile update function.	2023-03-15T14:15:11.783	2023-03-17T19:06:48.753
CVE-2023-24732	8.8	Simple Customer Relationship Management System v1.0 as discovered to contain a SQL injection vulnerability via the gender parameter in the user profile update function.	2023-03-15T14:15:11.833	2023-03-17T19:07:51.217
CVE-2022-38456	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Ernest Marcinko Ajax Search Lite plugin <= 4.10.3 versions.	2023-03-15T15:15:09.357	2023-03-17T17:39:43.797
CVE-2022-44580	8.8	SQL Injection (SQLi) vulnerability in RichPlugins Plugin for Google Reviews plugin <= 2.2.3 versions.	2023-03-15T15:15:09.447	2023-03-17T17:50:55.450

CVE-2023-27103	8.8	Libde265 v1.0.11 was discovered to contain a heap buffer overflow via the function derive_collocated_motion_vectors at motion.cc.	2023-03-15T15:15:09.670	2023-03-17T19:28:38.297
CVE-2023-27781	7.8	jpegoptim v1.5.2 was discovered to contain a heap overflow in the optimize function at jpegoptim.c.	2023-03-15T15:15:09.733	2023-03-17T19:26:47.957
CVE-2023-1415	6.3	A vulnerability was found in Simple Art Gallery 1.0. It has been declared as critical. This vulnerability affects the function sliderPicSubmit of the file adminHome.php. The manipulation leads to unrestricted upload. The attack can be initiated remotely. VDB-223126 is the identifier assigned to this vulnerability.	2023-03-15T16:15:10.977	2023-03-17T19:35:36.057
CVE-2023-24229	7.8	DrayTek Vigor2960 v1.5.1.4 was discovered to contain a command injection vulnerability via the mainfunction.cgi component.	2023-03-15T18:15:10.460	2023-03-19T03:57:06.433
CVE-2023-26284	8.8	IBM MQ Certified Container 9.3.0.1 through 9.3.0.3 and 9.3.1.0 through 9.3.1.1 could allow authenticated users with the cluster to be granted administration access to the MQ console due to improper access controls. IBM X-Force ID: 248417.	2023-03-15T18:15:10.703	2023-03-19T03:52:55.130
CVE-2020-4927	8.2	A vulnerability in the Spectrum Scale 5.0.5.0 through 5.1.6.1 core component could allow unauthorized access to user data or injection of arbitrary data in the communication protocol. IBM X-Force ID: 191695.	2023-03-15T19:15:24.500	2023-03-19T03:54:37.027
CVE-2023-25345	7.5	Directory traversal vulnerability in swig-templates thru 2.0.4 and swig thru 1.4.2, allows attackers to read arbitrary files via the include or extends tags.	2023-03-15T20:15:10.533	2023-03-18T03:50:49.197
CVE-2023-26484	8.2	KubeVirt is a virtual machine management add-on for Kubernetes. In versions 0.59.0 and prior, if a malicious user has taken over a Kubernetes node where virt-handler (the KubeVirt node-daemon) is running, the virt-handler service account can be used to modify all node specs. This can be misused to lure-in system-level-privileged components which can, for instance, read all secrets on the cluster, or can exec into pods on other nodes. This way, a compromised node can be used to elevate privileges beyond the node until potentially having full privileged access to the whole cluster. The simplest way to exploit this, once a user could compromise a specific node, is to set with the virt-handler service account all other nodes to unschedulable and simply wait until system-critical components with high privileges appear on its node. No patches are available as of time of publication. As a workaround, gatekeeper users can add a webhook which will block the `virt-handler` service account to modify the spec of a node.	2023-03-15T21:15:08.857	2023-03-16T12:56:10.680

CVE-2023-27596	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.8 and 3.2.5, OpenSIPS crashes when a malformed SDP body is sent multiple times to an OpenSIPS configuration that makes use of the `stream_process` function. This issue was discovered during coverage guided fuzzing of the function `codec_delete_except_re`. By abusing this vulnerability, an attacker is able to crash the server. It affects configurations containing functions that rely on the affected code, such as the function `codec_delete_except_re`. This issue has been fixed in version 3.1.8 and 3.2.5.	2023-03-15T21:15:08.953	2023-03-21T19:14:50.977
CVE-2023-27597	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.8 and 3.2.5, when a specially crafted SIP message is processed by the function `rewrite_ruri`, a crash occurs due to a segmentation fault. This issue causes the server to crash. It affects configurations containing functions that make use of the affected code, such as the function `setport`. This issue has been fixed in version 3.1.8 and 3.2.5.	2023-03-15T21:15:09.057	2023-03-21T19:14:22.760
CVE-2023-27598	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, sending a malformed `Via` header to OpenSIPS triggers a segmentation fault when the function `calc_tag_suffix` is called. A specially crafted `Via` header, which is deemed correct by the parser, will pass uninitialized strings to the function `MD5StringArray` which leads to the crash. Abuse of this vulnerability leads to Denial of Service due to a crash. Since the uninitialized string points to memory location `0x0`, no further exploitation appears to be possible. No special network privileges are required to perform this attack, as long as the OpenSIPS configuration makes use of functions such as `sl_send_reply` or `sl_gen_totag` that trigger the vulnerable code. This issue has been fixed in versions 3.1.7 and 3.2.4.	2023-03-15T21:15:09.143	2023-03-21T19:14:05.020
CVE-2023-27599	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, when the function `append_hf` handles a SIP message with a malformed To header, a call to the function `abort()` is performed, resulting in a crash. This is due to the following check in `data_lump.c:399` in the function `anchor_lump`. An attacker abusing this vulnerability will crash OpenSIPS leading to Denial of Service. It affects configurations containing functions that make use of the affected code, such as the function `append_hf`. This issue has been fixed in versions 3.1.7 and 3.2.4.	2023-03-15T21:15:09.247	2023-03-21T19:13:17.753
CVE-2023-28450	7.5	An issue was discovered in Dnsmasq before 2.90. The default maximum EDNS.0 UDP packet size was set to 4096 but should be 1232 because of DNS Flag Day 2020.	2023-03-15T21:15:09.333	2023-03-21T19:24:15.060

CVE-2023-27600	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, OpenSIPS crashes when a malformed SDP body is received and is processed by the `delete_sdp_line` function in the sipmsgops module. This issue can be reproduced by calling the function with an SDP body that does not terminate by a line feed (i.e. `\\n`). The vulnerability was found while performing black-box fuzzing against an OpenSIPS server running a configuration that made use of the functions `codec_delete_except_re` and `codec_delete_re`. The same issue was also discovered while performing coverage guided fuzzing on the function `codec_delete_except_re`. The crash happens because the function `delete_sdp_line` expects that an SDP line is terminated by a line feed (`\\n`). By abusing this vulnerability, an attacker is able to crash the server. It affects configurations containing functions that rely on the affected code, such as the function `codec_delete_except_re`. Due to the sanity check that is performed in the `del_lump` function, exploitation of this issue will generate an `abort` in the lumps processing function, resulting in a Denial of Service. This issue is patched in versions 3.1.7 and 3.2.4.	2023-03-15T22:15:10.267	2023-03-21T19:23:58.160
CVE-2023-27601	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, OpenSIPS crashes when a malformed SDP body is received and is processed by the `delete_sdp_line` function in the sipmsgops module. This issue can be reproduced by calling the function with an SDP body that does not terminate by a line feed (i.e. `\\n`). The vulnerability was found while performing black-box fuzzing against an OpenSIPS server running a configuration that made use of the functions `codec_delete_except_re` and `codec_delete_re`. The same issue was also discovered while performing coverage guided fuzzing on the function `codec_delete_except_re`. The crash happens because the function `delete_sdp_line` expects that an SDP line is terminated by a line feed (`\\n`): By abusing this vulnerability, an attacker is able to crash the server. It affects configurations containing functions that rely on the affected code, such as the function `codec_delete_except_re`. Due to the sanity check that is performed in the `del_lump` function, exploitation of this issue will generate an `abort` in the lumps processing function, resulting in a Denial of Service. This issue has been fixed in versions 3.1.7 and 3.2.4.	2023-03-15T22:15:10.357	2023-03-21T19:23:40.770

CVE-2023-28095	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Versions prior to 3.1.7 and 3.2.4 have a potential issue in `msg_translator.c:2628` which might lead to a server crash. This issue was found while fuzzing the function `build_res_buf_from_sip_req` but could not be reproduced against a running instance of OpenSIPS. This issue could not be exploited against a running instance of OpenSIPS since no public function was found to make use of this vulnerable code. Even in the case of exploitation through unknown vectors, it is highly unlikely that this issue would lead to anything other than Denial of Service. This issue has been fixed in versions 3.1.7 and 3.2.4.	2023-03-15T22:15:10.440	2023-03-21T19:23:29.190
CVE-2023-28096	7.5	OpenSIPS, a Session Initiation Protocol (SIP) server implementation, has a memory leak starting in the 2.3 branch and priot to versions 3.1.8 and 3.2.5. The memory leak was detected in the function `parse_mi_request` while performing coverage-guided fuzzing. This issue can be reproduced by sending multiple requests of the form `{"jsonrpc": "2.0","method": "log_le`. This malformed message was tested against an instance of OpenSIPS via FIFO transport layer and was found to increase the memory consumption over time. To abuse this memory leak, attackers need to reach the management interface (MI) which typically should only be exposed on trusted interfaces. In cases where the MI is exposed to the internet without authentication, abuse of this issue will lead to memory exhaustion which may affect the underlying system's availability. No authentication is typically required to reproduce this issue. On the other hand, memory leaks may occur in other areas of OpenSIPS where the cJSON library is used for parsing JSON objects. The issue has been fixed in versions 3.1.8 and 3.2.5.	2023-03-15T22:15:10.527	2023-03-21T19:23:06.670
CVE-2023-1389	8.8	TP-Link Archer AX21 (AX1800) firmware versions before 1.1.4 Build 20230219 contained a command injection vulnerability in the country form of the /cgi-bin/luci;stok=/locale endpoint on the web management interface. Specifically, the country parameter of the write operation was not sanitized before being used in a call to popen(), allowing an unauthenticated attacker to inject commands, which would be run as root, with a simple POST request.	2023-03-15T23:15:09.403	2023-03-21T19:31:47.030
CVE-2023-28097	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.9 and 3.2.6, a malformed SIP message containing a large _Content-Length_ value and a specially crafted Request-URI causes a segmentation fault in OpenSIPS. This issue occurs when a large amount of shared memory using the `-m` flag was allocated to OpenSIPS, such as 10 GB of RAM. On the test system, this issue occurred when shared memory was set to `2362` or higher. This issue is fixed in versions 3.1.9 and 3.2.6. The only workaround is to guarantee that the Content-Length value of input messages is never larger than `2147483647`.	2023-03-15T23:15:09.627	2023-03-21T22:40:02.477

CVE-2023-28098	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, a specially crafted Authorization header causes OpenSIPS to crash or behave in an unexpected way due to a bug in the function `parse_param_name()` . This issue was discovered while performing coverage guided fuzzing of the function parse_msg. The AddressSanitizer identified that the issue occurred in the function `q_memchr()` which is being called by the function `parse_param_name()`. This issue may cause erratic program behaviour or a server crash. It affects configurations containing functions that make use of the affected code, such as the function `www_authorize()` . Versions 3.1.7 and 3.2.4 contain a fix.	2023-03-15T23:15:09.717	2023-03-21T22:39:28.990
CVE-2023-28099	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.9 and 3.2.6, if `ds_is_in_list()` is used with an invalid IP address string (`NULL` is illegal input), OpenSIPS will attempt to print a string from a random address (stack garbage), which could lead to a crash. All users of `ds_is_in_list()` without the `$si` variable as 1st parameter could be affected by this vulnerability to a larger, lesser or no extent at all, depending if the data passed to the function is a valid IPv4 or IPv6 address string or not. Fixes will are available starting with the 3.1.9 and 3.2.6 minor releases. There are no known workarounds.	2023-03-15T23:15:09.807	2023-03-21T22:39:07.327
CVE-2023-28337	8.8	When uploading a firmware image to a Netgear Nighthawk Wifi6 Router (RAX30), a hidden “forceFWUpdate” parameter may be provided to force the upgrade to complete and bypass certain validation checks. End users can use this to upload modified, unofficial, and potentially malicious firmware to the device.	2023-03-15T23:15:09.897	2023-03-21T17:40:15.477
CVE-2023-28338	7.5	"Any request send to a Netgear Nighthawk Wifi6 Router (RAX30)s web service containing a “Content-Type” of “multipartboundary=” will result in the request body being written to “/tmp/mulipartFile” on the device itself. A sufficiently large file will cause device resources to be exhausted, resulting in the device becoming unusable until it is rebooted.	2023-03-15T23:15:09.957	2023-03-21T17:57:33.130
CVE-2023-28466	7.0	do_tls_getsockopt in net/tls/tls_main.c in the Linux kernel through 6.2.6 lacks a lock_sock call, leading to a race condition (with a resultant use-after-free or NULL pointer dereference).	2023-03-16T00:15:11.563	2023-03-21T17:27:19.377
CVE-2023-25281	7.5	A stack overflow vulnerability exists in pingV4Msg component in D-Link DIR820LA1_FW105B03, allows attackers to cause a denial of service via the nextPage parameter to ping.ccp.	2023-03-16T01:15:46.857	2023-03-21T17:46:30.813
CVE-2023-24760	8.8	An issue found in Ofcms v.1.1.4 allows a remote attacker to to escalate privileges via the respwd method in SysUserController.	2023-03-16T02:15:08.387	2023-03-21T18:31:35.910

CVE-2022-4009	8.8	In affected versions of Octopus Deploy it is possible for a user to introduce code via offline package creation	2023-03-16T04:15:12.167	2023-03-21T18:43:26.053
CVE-2022-38063	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Social Login WP plugin <= 5.0.0.0 versions.	2023-03-16T09:15:09.090	2023-03-21T18:35:55.460
CVE-2022-34406	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:09.910	2023-03-16T12:55:47.417
CVE-2022-34407	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:09.990	2023-03-16T12:55:47.417
CVE-2022-34408	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:10.060	2023-03-16T12:55:47.417
CVE-2022-34409	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:10.137	2023-03-16T12:55:47.417
CVE-2022-34410	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:10.210	2023-03-16T12:55:47.417
CVE-2022-34411	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:10.280	2023-03-16T12:55:47.417
CVE-2022-34412	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:10.353	2023-03-16T12:55:47.417
CVE-2022-34413	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:10.427	2023-03-16T12:55:47.417

CVE-2022-34414	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:10.500	2023-03-16T12:55:47.417
CVE-2022-34415	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:10.570	2023-03-16T12:55:47.417
CVE-2022-34416	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:10.643	2023-03-16T12:55:47.417
CVE-2022-34417	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:10.717	2023-03-16T12:55:47.417
CVE-2022-34418	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:10.790	2023-03-16T12:55:47.417
CVE-2022-34419	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:10.860	2023-03-16T12:55:47.417
CVE-2022-34420	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:10.933	2023-03-16T12:55:47.417
CVE-2022-34421	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:11.007	2023-03-16T12:55:47.417
CVE-2022-34422	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T12:15:11.093	2023-03-16T12:55:47.417
CVE-2022-34423	7.5	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	2023-03-16T13:15:10.137	2023-03-16T15:17:42.803

CVE-2023-1433	4.7	A vulnerability was found in SourceCodester Gadget Works Online Ordering System 1.0. It has been classified as problematic. This affects an unknown part of the file admin/products/controller.php?action=add of the component Products Handler. The manipulation of the argument filename leads to unrestricted upload. It is possible 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-223215.	2023-03-16T13:15:10.407	2023-03-22T02:39:04.040
CVE-2023-27875	7.5	"IBM Aspera Faspex 5.0.4 could allow a user to change other users credentials due to improper access controls. IBM X-Force ID: 249847.	2023-03-16T13:15:10.543	2023-03-22T00:57:46.697
CVE-2021-31637	7.8	An issue found in UwAmp v.1.1, 1.2, 1.3, 2.0, 2.1, 2.2, 2.2.1, 3.0.0, 3.0.1, 3.0.2 allows a remote attacker to execute arbitrary code via a crafted DLL.	2023-03-16T15:15:10.053	2023-03-22T01:32:09.007
CVE-2023-26767	7.5	Buffer Overflow vulnerability found in Liblouis v.3.24.0 allows a remote attacker to cause a denial of service via the lou_logFile function at logginc.c endpoint.	2023-03-16T15:15:10.233	2023-03-22T02:01:04.683
CVE-2023-26768	7.5	Buffer Overflow vulnerability found in Liblouis v.3.24.0 allows a remote attacker to cause a denial of service via the compileTranslationTable.c and lou_setDataPath functions.	2023-03-16T15:15:10.290	2023-03-22T02:03:01.407
CVE-2023-26769	7.5	Buffer Overflow vulnerability found in Liblouis Lou_Trace v.3.24.0 allows a remote attacker to cause a denial of service via the resolveSubtable function at compileTranslationTabel.c.	2023-03-16T15:15:10.343	2023-03-22T02:07:37.703
CVE-2023-27037	8.8	Qibosoft QiboCMS v7 was discovered to contain a remote code execution (RCE) vulnerability via the Get_Title function at label_set_rs.php	2023-03-16T15:15:10.407	2023-03-22T01:49:28.147
CVE-2023-27707	7.2	SQL injection vulnerability found in DedeCMS v.5.7.106 allows a remote attacker to execute arbitrary code via the rank_* parameter in the /dede/group_store.php endpoint.	2023-03-16T15:15:10.557	2023-03-22T02:23:37.980
CVE-2023-27709	7.2	SQL injection vulnerability found in DedeCMS v.5.7.106 allows a remote attacker to execute arbitrary code via the rank_* parameter in the /dedestory_catalog.php endpoint.	2023-03-16T15:15:10.607	2023-03-22T02:29:25.080
CVE-2023-28104	7.5	`silverstripe/graphql` serves Silverstripe data as GraphQL representations. In versions 4.2.2 and 4.1.1, an attacker could use a specially crafted graphql query to execute a denial of service attack against a website which has a publicly exposed graphql endpoint. This mostly affects websites with particularly large/complex graphql schemas. Users should upgrade to `silverstripe/graphql` 4.2.3 or 4.1.2 to remedy the vulnerability.	2023-03-16T16:15:12.750	2023-03-16T18:40:56.770

CVE-2023-28105	8.8	go-used-util has commonly used utility functions for Go. Versions prior to 0.0.34 have a ZipSlip issue when using fsutil package to unzip files. When users use `zip.Unzip` to unzip zip files from a malicious attacker, they may be vulnerable to path traversal. The issue has been fixed in version 0.0.34. There are no known workarounds.	2023-03-16T17:15:09.483	2023-03-16T18:40:56.770
CVE-2023-28108	7.9	Pimcore is an open source data and experience management platform. Prior to version 10.5.19, quoting is not done properly in UUID DAO model. There is the theoretical possibility to inject custom SQL if the developer is using this methods with input data and not doing proper input validation in advance and so relies on the auto-quoting being done by the DAO class. Users should update to version 10.5.19 to receive a patch or, as a workaround, apply the patch manually.	2023-03-16T17:15:09.663	2023-03-16T18:40:56.770
CVE-2023-0598	7.8	GE Digital Proficy iFIX 2022, GE Digital Proficy iFIX v6.1, and GE Digital Proficy iFIX v6.5 are vulnerable to code injection, which may allow an attacker to insert malicious configuration files in the expected web server execution path and gain full control of the HMI software.	2023-03-16T20:15:11.327	2023-03-17T04:04:43.147
CVE-2022-43441	8.1	A code execution vulnerability exists in the Statement Bindings functionality of Ghost Foundation node-sqlite3 5.1.1. A specially-crafted Javascript file can lead to arbitrary code execution. An attacker can provide malicious input to trigger this vulnerability.	2023-03-16T21:15:11.023	2023-03-17T04:04:43.147
CVE-2022-43606	7.5	A use-of-uninitialized-pointer vulnerability exists in the Forward Open connection_management_entry functionality of EIP Stack Group OpENer development commit 58ee13c. A specially-crafted EtherNet/IP request can lead to use of a null pointer, causing the server to crash. An attacker can send a series of EtherNet/IP requests to trigger this vulnerability.	2023-03-16T21:15:11.277	2023-03-17T04:04:43.147
CVE-2023-22883	7.2	Zoom Client for IT Admin Windows installers before version 5.13.5 contain a local privilege escalation vulnerability. A local low-privileged user could exploit this vulnerability in an attack chain during the installation process to escalate their privileges to the SYSTEM user.	2023-03-16T21:15:13.107	2023-03-17T04:04:43.147
CVE-2021-21548	7.4	"Dell EMC Unisphere for PowerMax versions before 9.1.0.27, Dell EMC Unisphere for PowerMax Virtual Appliance versions before 9.1.0.27, and PowerMax OS Release 5978 contain an improper certificate validation vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability to carry out a man-in-the-middle attack by supplying a crafted certificate and intercepting the victims traffic to view or modify a victim's data in transit.	2023-03-17T06:15:51.937	2023-03-17T12:59:31.617

CVE-2023-1444	7.5	A vulnerability was found in Filseclab Twister Antivirus 8. It has been rated as critical. This issue affects some unknown processing in the library fildds.sys of the component IoControlCode Handler. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223289 was assigned to this vulnerability.	2023-03-17T07:15:11.083	2023-03-17T12:59:31.617
CVE-2023-1464	7.3	A vulnerability, which was classified as critical, was found in SourceCodester Medicine Tracker System 1.0. This affects an unknown part of the file Users.php?f=save_user. The manipulation of the argument firstname/middlename/lastname/username/password leads to improper authentication. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-223311.	2023-03-17T12:15:11.987	2023-03-17T12:59:25.697
CVE-2023-1172	7.2	The Bookly plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the full name value in versions up to, and including, 21.5 due to insufficient input 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.	2023-03-17T13:15:10.463	2023-03-17T15:44:01.930
CVE-2023-1471	8.8	"The WP Popup Banners plugin for WordPress is vulnerable to SQL Injection via the banner_id parameter in versions up to, and including, 1.2.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with minimal permissions, such as a subscrber, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2023-03-17T14:15:12.347	2023-03-17T15:44:01.930
CVE-2023-27591	7.5	Miniflux is a feed reader. Prior to version 2.0.43, an unauthenticated user can retrieve Prometheus metrics from a publicly reachable Miniflux instance where the `METRICS_COLLECTOR` configuration option is enabled and `METRICS_ALLOWED_NETWORKS` is set to `127.0.0.1/8` (the default). A patch is available in Miniflux 2.0.43. As a workaround, set `METRICS_COLLECTOR` to `false` (default) or run Miniflux behind a trusted reverse-proxy.	2023-03-17T20:15:13.100	2023-03-20T02:46:58.537

CVE-2023-28116	8.1	Contiki-NG is an open-source, cross-platform operating system for internet of things (IoT) devices. In versions 4.8 and prior, an out-of-bounds write can occur in the BLE L2CAP module of the Contiki-NG operating system. The network stack of Contiki-NG uses a global buffer (packetbuf) for processing of packets, with the size of PACKETBUF_SIZE. In particular, when using the BLE L2CAP module with the default configuration, the PACKETBUF_SIZE value becomes larger then the actual size of the packetbuf. When large packets are processed by the L2CAP module, a buffer overflow can therefore occur when copying the packet data to the packetbuf. The vulnerability has been patched in the "develop" branch of Contiki-NG, and will be included in release 4.9. The problem can be worked around by applying the patch manually.	2023-03-17T22:15:11.547	2023-03-20T02:46:58.537
CVE-2023-26113	7.5	Versions of the package collection.js before 6.8.1 are vulnerable to Prototype Pollution via the extend function in Collection.js/dist/node/iterators/extend.js.	2023-03-18T05:15:52.937	2023-03-20T02:46:58.537
CVE-2023-1489	7.8	A vulnerability has been found in Lespeed WiseCleaner Wise System Monitor 1.5.3.54 and classified as critical. Affected by this vulnerability is an unknown functionality in the library WiseHDInfo64.dll of the component IoControlCode Handler. The manipulation leads to improper access controls. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223375.	2023-03-18T22:15:11.440	2023-03-20T02:46:58.537
CVE-2023-1250	7.4	Improper Input Validation vulnerability in OTRS AG OTRS (ACL modules), OTRS AG ((OTRS)) Community Edition (ACL modules) allows Local Execution of Code. When creating/importing an ACL it was possible to inject code that gets executed via manipulated comments and ACL-names This issue affects OTRS: from 7.0.X before 7.0.42, from 8.0.X before 8.0.31; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34.	2023-03-20T09:15:12.020	2023-03-20T14:02:42.383
CVE-2022-47592	7.1	Reflected Cross-Site Scripting (XSS) vulnerability in Dmytriy.Cooperman MagicForm plugin <= 0.1 versions.	2023-03-20T12:15:10.973	2023-03-20T14:02:37.427
CVE-2023-22682	7.1	Reflected Cross-Site Scripting (XSS) vulnerability in Manuel Masia | Pixedelic.Com Camera slideshow plugin <= 1.4.0.1 versions.	2023-03-20T12:15:11.427	2023-03-20T14:02:37.427
CVE-2022-47591	7.1	Reflected Cross-Site Scripting (XSS) vulnerability in Mickael Austoni Map Multi Marker plugin <= 3.2.1 versions.	2023-03-20T13:15:11.557	2023-03-20T14:02:37.427
CVE-2023-26513	7.5	Excessive Iteration vulnerability in Apache Software Foundation Apache Sling Resource Merger.This issue affects Apache Sling Resource Merger: from 1.2.0 before 1.4.2.	2023-03-20T13:15:11.783	2023-03-20T14:02:37.427

CVE-2023-28118	7.5	kaml provides YAML support for kotlinx.serialization. Prior to version 0.53.0, applications that use kaml to parse untrusted input containing anchors and aliases may consume excessive memory and crash. Version 0.53.0 and later default to refusing to parse YAML documents containing anchors and aliases. There are no known workarounds.	2023-03-20T13:15:11.877	2023-03-20T14:02:37.427
CVE-2022-43663	8.1	An integer conversion vulnerability exists in the SORBAx64.dll RecvPacket functionality of WellinTech KingHistorian 35.01.00.05. A specially crafted network packet can lead to a buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.	2023-03-20T21:15:10.533	2023-03-21T11:51:09.643
CVE-2022-45124	7.5	An information disclosure vulnerability exists in the User authentication functionality of WellinTech KingHistorian 35.01.00.05. A specially crafted network packet can lead to a disclosure of sensitive information. An attacker can sniff network traffic to leverage this vulnerability.	2023-03-20T21:15:10.647	2023-03-21T11:51:09.643
CVE-2012-10009	7.3	A vulnerability was found in 404like Plugin up to 1.0.2. It has been classified as critical. Affected is the function checkPage of the file 404Like.php. The manipulation of the argument searchWord leads to sql injection. It is possible to launch the attack remotely. Upgrading to version 1.0.2 is able to address this issue. The name of the patch is 2c4b589d27554910ab1fd104ddbec9331b540f7f. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-223404.	2023-03-21T00:15:10.163	2023-03-21T11:51:09.643
CVE-2023-1527	8.3	Cross-site Scripting (XSS) - Generic in GitHub repository tsolucio/corebos prior to 8.0.	2023-03-21T00:15:10.780	2023-03-21T11:51:09.643
CVE-2023-1535	8.3	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.7.	2023-03-21T05:15:08.797	2023-03-21T11:51:09.643
CVE-2023-1536	7.6	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.7.	2023-03-21T05:15:09.630	2023-03-21T11:51:03.997
CVE-2023-1542	8.1	Business Logic Errors in GitHub repository answerdev/answer prior to 1.0.6.	2023-03-21T05:15:10.160	2023-03-21T11:51:03.997
CVE-2023-27980	8.8	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior)	2023-03-21T06:15:13.063	2023-03-21T11:51:03.997

CVE-2023-27982	8.8	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).	2023-03-21T07:15:08.410	2023-03-21T11:51:03.997
CVE-2023-1462	8.5	Authorization Bypass Through User-Controlled Key vulnerability in Vadi Corporate Information Systems DigiKent allows Authentication Bypass, Authentication Abuse. This issue affects DigiKent: before 23.03.20.	2023-03-21T09:15:10.497	2023-03-21T11:51:03.997
CVE-2023-27978	7.8	A CWE-502: Deserialization of Untrusted Data vulnerability exists in the Dashboard module that could cause an interpretation of malicious payload data, potentially leading to remote code execution when an attacker gets the user to open a malicious file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).	2023-03-21T09:15:11.470	2023-03-21T11:51:03.997
CVE-2023-27981	7.8	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).	2023-03-21T10:15:17.173	2023-03-21T11:51:03.997
CVE-2023-1545	7.5	SQL Injection in GitHub repository nilsteampassnet/teampass prior to 3.0.0.23.	2023-03-21T11:15:10.453	2023-03-21T11:51:03.997
CVE-2023-27984	7.8	A CWE-20: Improper Input Validation vulnerability exists in Custom Reports that could cause a macro to be executed, potentially leading to remote code execution when a user opens a malicious report file planted by an attacker. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).	2023-03-21T11:15:10.553	2023-03-21T11:51:03.997

CVE-2023-1314	7.5	"A vulnerability has been discovered in cloudflareds installer (<= 2023.3.0) for Windows 32-bits devices that allows a local attacker with no administrative permissions to escalate their privileges on the affected device. This vulnerability exists because the MSI installer used by cloudflared relied on a world-writable directory. An attacker with local access to the device (without Administrator rights) can use symbolic links to trick the MSI installer into deleting files in locations that the attacker would otherwise have no access to. By creating a symlink from the world-writable directory to the target file, the attacker can manipulate the MSI installers repair functionality to delete the target file during the repair process. Exploitation of this vulnerability could allow an attacker to delete important system files or replace them with malicious files, potentially leading to the affected device being compromised. The cloudflared client itself is not affected by this vulnerability, only the installer for 32-bit Windows devices.	2023-03-21T12:15:10.563	2023-03-21T12:19:40.680
CVE-2023-27871	7.5	IBM Aspera Faspex 4.4.2 could allow a remote attacker to obtain sensitive credential information for an external user, using a specially crafted SQL query. IBM X-Force ID: 249613.	2023-03-21T15:15:12.477	2023-03-21T17:00:14.450
CVE-2022-36429	7.2	A command execution vulnerability exists in the ubus backend communications functionality of Netgear Orbi Satellite RBS750 4.6.8.5. A specially-crafted JSON object can lead to arbitrary command execution. An attacker can send a sequence of malicious packets to trigger this vulnerability.	2023-03-21T18:15:11.970	2023-03-21T20:07:21.987
CVE-2022-38452	7.2	A command execution vulnerability exists in the hidden telnet service functionality of Netgear Orbi Router RBR750 4.6.8.5. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a network request to trigger this vulnerability.	2023-03-21T18:15:12.193	2023-03-21T20:07:21.987
CVE-2023-1261	8.2	Missing MAC layer security in Silicon Labs Wi-SUN SDK v1.5.0 and earlier allows malicious node to route malicious messages through network.	2023-03-21T21:15:12.097	2023-03-21T22:40:42.437
CVE-2023-1262	8.2	Missing MAC layer security in Silicon Labs Wi-SUN Linux Border Router v1.5.2 and earlier allows malicious node to route malicious messages through network.	2023-03-21T21:15:12.220	2023-03-21T22:40:42.437
CVE-2023-26497	8.6	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute.	2023-03-21T22:15:12.210	2023-03-21T22:40:42.437
CVE-2023-27856	7.5	"In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automations ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed.	2023-03-22T00:15:12.810	2023-03-22T12:48:04.240

CVE-2023-27857	7.5	"In affected versions, a heap-based buffer over-read condition occurs when the message field indicates more data than is present in the message field in Rockwell Automations ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to crash ThinServer.exe due to a read access violation.	2023-03-22T02:15:48.953	2023-03-22T12:48:04.240
CVE-2023-1168	7.2	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX.	2023-03-22T06:15:09.390	2023-03-22T12:48:04.240
CVE-2023-1370	7.5	[Json-smart](https://netplex.github.io/json-smart/) is a performance focused, JSON processor lib. When reaching a '[' or '{' character in the JSON input, the code parses an array or an object respectively. It was discovered that the code does not have any limit to the nesting of such arrays or objects. Since the parsing of nested arrays and objects is done recursively, nesting too many of them can cause a stack exhaustion (stack overflow) and crash the software.	2023-03-22T06:15:09.493	2023-03-22T12:48:04.240
CVE-2023-25590	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance.	2023-03-22T06:15:09.927	2023-03-22T12:47:56.330
CVE-2023-25591	7.6	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow a remote attacker authenticated with low privileges to access sensitive information. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further privileges on the ClearPass instance.	2023-03-22T06:15:10.017	2023-03-22T12:47:56.330
CVE-2023-25592	7.1	"Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victims browser in the context of the affected interface.	2023-03-22T06:15:10.110	2023-03-22T12:47:56.330
CVE-2023-25593	7.1	"Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victims browser in the context of the affected interface.	2023-03-22T06:15:10.220	2023-03-22T12:47:56.330

CVE-2023-28083	8.3	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out.	2023-03-22T06:15:10.950	2023-03-22T12:47:56.330