Vulnerabilidades Publicadas Na Semana

Vulnerabilidades de Severidade Crítica

ID	CVSS Score	Descrição	Publicado em	Última Modificação
CVE-2021-3854	9.8	[{'lang': 'en', 'value': "Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Glox Technology Useroam Hotspot allows SQL Injection. This issue affects Useroam Hotspot: before 5.1.0.15."}]	2023-03-02T12:15:08.957	2023-03-02T13:46:06.947
CVE-2023-26477	10.0	[{'lang': 'en', 'value': "XWiki Platform is a generic wiki platform. Starting in versions 6.3-rc-1 and 6.2.4, it's possible to inject arbitrary wiki syntax including Groovy, Python and Velocity script macros via the `newThemeName` request parameter (URL parameter), in combination with additional parameters. This has been patched in the supported versions 13.10.10, 14.9-rc-1, and 14.4.6. As a workaround, it is possible to edit `FlamingoThemesCode.WebHomeSheet` and manually perform the changes from the patch fixing the issue."}]	2023-03-02T18:15:10.293	2023-03-02T18:22:34.447
CVE-2023-26055	9.9	[{'lang': 'en', 'value': 'XWiki Commons are technical libraries common to several other top level XWiki projects. Starting in version 3.1-milestone-1, any user can edit their own profile and inject code, which is going to be executed with programming right. The same vulnerability can also be exploited in all other places where short text properties are displayed, e.g., in apps created using Apps Within Minutes that use a short text field. The problem has been patched on versions 13.10.9, 14.4.4, 14.7RC1.'}]	2023-03-02T19:15:10.867	2023-03-02T20:11:16.100
CVE-2023-26471	9.9	[{'lang': 'en', 'value': 'XWiki Platform is a generic wiki platform. Starting in version 11.6-rc-1, comments are supposed to be executed with the right of superadmin but in restricted mode (anything dangerous is disabled), but the async macro does not take into account the restricted mode. This means that any user with comment right can use the async macro to make it execute any wiki content with the right of superadmin. This has been patched in XWiki 14.9, 14.4.6, and 13.10.10. The only known workaround consists of applying a patch and rebuilding and redeploying `org.xwiki.platform:xwiki-platform-rendering-async-macro`.'}]	2023-03-02T19:15:11.137	2023-03-02T20:11:16.100
CVE-2023-26472	9.9	[{'lang': 'en', 'value': 'XWiki Platform is a generic wiki platform. Starting in version 6.2-milestone-1, one can execute any wiki content with the right of IconThemeSheet author by creating an icon theme with certain content. This can be done by creating a new page or even through the user profile for users not having edit right. The issue has been patched in XWiki 14.9, 14.4.6, and 13.10.10. An available workaround is to fix the bug in the page `IconThemesCode.IconThemeSheet` by applying a modification from commit 48caf7491595238af2b531026a614221d5d61f38.'}]	2023-03-02T19:15:11.220	2023-03-02T20:11:16.100
CVE-2023-26474	9.9	[{'lang': 'en', 'value': "XWiki Platform is a generic wiki platform. Starting in version 13.10, it's possible to use the right of an existing document content author to execute a text area property. This has been patched in XWiki 14.10, 14.4.7, and 13.10.11. There are no known workarounds."}]	2023-03-02T19:15:11.390	2023-03-02T20:11:16.100
CVE-2023-26475	9.9	[{'lang': 'en', 'value': 'XWiki Platform is a generic wiki platform. Starting in version 2.3-milestone-1, the annotation displayer does not execute the content in a restricted context. This allows executing anything with the right of the author of any document by annotating the document. This has been patched in XWiki 13.10.11, 14.4.7 and 14.10. There is no easy workaround except to upgrade.'}]	2023-03-02T19:15:11.470	2023-03-02T20:11:16.100
CVE-2023-20078	9.8	[{'lang': 'en', 'value': 'Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory.'}]	2023-03-03T16:15:10.277	2023-03-03T17:15:10.700
CVE-2023-20079	9.8	[{'lang': 'en', 'value': 'Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory.'}]	2023-03-03T16:15:10.380	2023-03-03T17:15:10.790
CVE-2023-27290	9.1	[{'lang': 'en', 'value': 'Docker based datastores for IBM Instana (IBM Observability with Instana 239-0 through 239-2, 241-0 through 241-2, and 243-0) do not currently require authentication. Due to this, an attacker within the network could access the datastores with read/write access. IBM X-Force ID: 248737.'}]	2023-03-03T23:15:12.580	2023-03-06T04:17:51.150
CVE-2023-26481	9.1	[{'lang': 'en', 'value': "authentik is an open-source Identity Provider. Due to an insufficient access check, a recovery flow link that is created by an admin (or sent via email by an admin) can be used to set the password for any arbitrary user. This attack is only possible if a recovery flow exists, which has both an Identification and an Email stage bound to it. If the flow has policies on the identification stage to skip it when the flow is restored (by checking `request.context['is_restored']`), the flow is not affected by this. With this flow in place, an administrator must create a recovery Link or send a recovery URL to the attacker, who can, due to the improper validation of the token create, set the password for any account. Regardless, for custom recovery flows it is recommended to add a policy that checks if the flow is restored, and skips the identification stage. This issue has been fixed in versions 2023.2.3, 2023.1.3 and 2022.12.2."}]	2023-03-04T01:15:10.447	2023-03-06T04:17:51.150
CVE-2023-0839	10.0	[{'lang': 'en', 'value': 'Improper Protection for Outbound Error Messages and Alert Signals vulnerability in ProMIS Process Co. InSCADA allows Account Footprinting.This issue affects inSCADA: before 20230115-1.'}]	2023-03-06T08:15:08.330	2023-03-06T13:41:36.803
CVE-2023-0979	9.8	[{'lang': 'en', 'value': "Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in MedData Informatics MedDataPACS.This issue affects MedDataPACS : before 2023-03-03."}]	2023-03-06T15:15:10.077	2023-03-06T19:14:23.420
CVE-2023-1244	9.3	[{'lang': 'en', 'value': 'Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6.'}]	2023-03-07T08:15:09.937	2023-03-07T13:54:09.087
CVE-2022-3760	9.8	[{'lang': 'en', 'value': "Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mia Technology Mia-Med.This issue affects Mia-Med: before 1.0.0.58."}]	2023-03-07T09:15:08.623	2023-03-07T13:54:09.087
CVE-2023-27479	9.9	[{'lang': 'en', 'value': 'XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with view rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of UIX parameters. A proof of concept exploit is to log in, add an `XWiki.UIExtensionClass` xobject to the user profile page, with an Extension Parameters content containing `label={{/html}} {{async async="true" cached="false" context="doc.reference"}}{{groovy}}println("Hello " + "from groovy!") {{/groovy}}{{/async}}`. Then, navigating to `PanelsCode.ApplicationsPanelConfigurationSheet` (i.e., `/xwiki/bin/view/PanelsCode/ApplicationsPanelConfigurationSheet` where `` is the URL of your XWiki installation) should not execute the Groovy script. If it does, you will see `Hello from groovy!` displayed on the screen. This vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10-rc-1. Users are advised to upgrade. For users unable to upgrade the issue can be fixed by editing the `PanelsCode.ApplicationsPanelConfigurationSheet` wiki page and making the same modifications as shown in commit `6de5442f3c`.'}]	2023-03-07T19:15:12.577	2023-03-07T20:14:26.217
CVE-2023-1267	9.8	[{'lang': 'en', 'value': "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	2023-03-08T13:55:55.097
CVE-2023-27482	10.0	[{'lang': 'en', 'value': '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	2023-03-08T19:47:01.990
CVE-2023-26489	9.9	[{'lang': 'en', 'value': "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 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."}]	2023-03-08T20:15:09.583	2023-03-08T20:15:09.583
CVE-2023-1283	10.0	[{'lang': 'en', 'value': 'Code Injection in GitHub repository builderio/qwik prior to 0.21.0.'}]	2023-03-08T22:15:09.683	2023-03-08T23:15:11.033
CVE-2023-1251	9.8	[{'lang': 'en', 'value': "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	2023-03-09T08:15:08.553

Vulnerabilidades de Severidade Alta

ID	CVSS Score	Descrição	Publicado em	Última modificação
CVE-2023-26480	8.9	[{'lang': 'en', 'value': 'XWiki Platform is a generic wiki platform. Starting in version 12.10, a user without script rights can introduce a stored cross-site scripting by using the Live Data macro. This has been patched in XWiki 14.9, 14.4.7, and 13.10.10. There are no known workarounds.'}]	2023-03-02T18:15:11.407	2023-03-02T18:22:34.447
CVE-2023-0084	7.2	[{'lang': 'en', 'value': 'The Metform Elementor Contact Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via text areas on forms in versions up to, and including, 3.1.2 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, which is the submissions page.'}]	2023-03-02T19:15:10.383	2023-03-02T20:11:16.100
CVE-2023-26476	7.5	[{'lang': 'en', 'value': 'XWiki Platform is a generic wiki platform. Starting in version 3.2-m3, users can deduce the content of the password fields by repeated call to `LiveTableResults` and `WikisLiveTableResultsMacros`. The issue can be fixed by upgrading to versions 14.7-rc-1, 13.4.4, or 13.10.9 and higher, or in version >= 3.2M3 by applying the patch manually on `LiveTableResults` and `WikisLiveTableResultsMacros`.'}]	2023-03-02T19:15:11.567	2023-03-02T20:11:16.100
CVE-2023-0457	7.5	[{'lang': 'en', 'value': 'Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server.'}]	2023-03-03T05:15:12.037	2023-03-03T13:52:55.773
CVE-2023-1164	8.4	[{'lang': 'en', 'value': 'A vulnerability was found in KylinSoft kylin-activation and classified as critical. Affected by this issue is some unknown functionality of the component File Import. The manipulation leads to improper authorization. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 1.3.11-23 and 1.30.10-5.p23 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-222260.'}]	2023-03-03T07:15:09.370	2023-03-03T15:15:11.047
CVE-2023-0957	8.2	[{'lang': 'en', 'value': 'An issue was discovered in Gitpod versions prior to release-2022.11.2.16. There is a Cross-Site WebSocket Hijacking (CSWSH) vulnerability that allows attackers to make WebSocket connections to the Gitpod JSONRPC server using a victim's credentials, because the Origin header is not restricted. This can lead to the extraction of data from workspaces, to a full takeover of the workspace.'}]	2023-03-03T08:15:08.613	2023-03-03T13:52:55.773
CVE-2023-1170	7.3	[{'lang': 'en', 'value': 'Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1376.'}]	2023-03-03T23:15:11.830	2023-03-06T04:17:51.150
CVE-2023-23929	8.8	[{'lang': 'en', 'value': 'vantage6 is a privacy preserving federated learning infrastructure for secure insight exchange. Currently, the refresh token is valid indefinitely. The refresh token should get a validity of 24-48 hours. A fix was released in version 3.8.0.'}]	2023-03-04T00:15:15.380	2023-03-06T04:17:51.150
CVE-2023-26490	7.3	[{'lang': 'en', 'value': 'mailcow is a dockerized email package, with multiple containers linked in one bridged network. The Sync Job feature - which can be made available to standard users by assigning them the necessary permission - suffers from a shell command injection. A malicious user can abuse this vulnerability to obtain shell access to the Docker container running dovecot. The imapsync Perl script implements all the necessary functionality for this feature, including the XOAUTH2 authentication mechanism. This code path creates a shell command to call openssl. However, since different parts of the specified user password are included without any validation, one can simply execute additional shell commands. Notably, the default ACL for a newly-created mailcow account does not include the necessary permission. The Issue has been fixed within the 2023-03 Update (March 3rd 2023). As a temporary workaround the Syncjob ACL can be removed from all mailbox users, preventing from creating or changing existing Syncjobs.'}]	2023-03-04T00:15:15.647	2023-03-06T04:17:51.150
CVE-2023-1175	7.3	[{'lang': 'en', 'value': 'Incorrect Calculation of Buffer Size in GitHub repository vim/vim prior to 9.0.1378.'}]	2023-03-04T16:15:09.533	2023-03-06T04:17:51.150
CVE-2023-0734	7.3	[{'lang': 'en', 'value': 'Improper Authorization in GitHub repository wallabag/wallabag prior to 2.5.4.'}]	2023-03-05T21:15:10.027	2023-03-06T04:17:51.150
CVE-2023-26106	7.5	[{'lang': 'en', 'value': 'All versions of the package dot-lens are vulnerable to Prototype Pollution via the set() function in index.js file.'}]	2023-03-06T05:15:12.200	2023-03-06T13:41:36.803
CVE-2023-26111	7.5	[{'lang': 'en', 'value': 'All versions of the package @nubosoftware/node-static; all versions of the package node-static are vulnerable to Directory Traversal due to improper file path sanitization in the startsWith() method in the servePath function.'}]	2023-03-06T05:15:12.920	2023-03-06T13:41:36.803
CVE-2023-22856	8.5	[{'lang': 'en', 'value': 'A stored Cross-site Scripting (XSS) vulnerability in BlogEngine.NET 3.3.8.0, allows injection of arbitrary JavaScript in the security context of a blog visitor through an upload of a specially crafted file.'}]	2023-03-06T07:15:11.363	2023-03-06T13:41:36.803
CVE-2023-22857	8.5	[{'lang': 'en', 'value': 'A stored Cross-site Scripting (XSS) vulnerability in BlogEngine.NET 3.3.8.0, allows injection of arbitrary JavaScript in the security context of a blog visitor through an injection of a malicious payload into a blog post.'}]	2023-03-06T07:15:11.757	2023-03-06T13:41:36.803
CVE-2022-2178	7.5	[{'lang': 'en', 'value': 'Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Saysis Computer Starcities. This issue affects Starcities: before 1.1.'}]	2023-03-06T12:15:08.803	2023-03-06T13:41:36.803
CVE-2023-27474	8.0	[{'lang': 'en', 'value': 'Directus is a real-time API and App dashboard for managing SQL database content. Instances relying on an allow-listed reset URL are vulnerable to an HTML injection attack through the use of query parameters in the reset URL. An attacker could exploit this to email users urls to the servers domain but which may contain malicious code. The problem has been resolved and released under version 9.23.0. People relying on a custom password reset URL should upgrade to 9.23.0 or later, or remove the custom reset url from the configured allow list. Users are advised to upgrade. Users unable to upgrade may disable the custom reset URL allow list as a workaround.'}]	2023-03-06T17:15:10.740	2023-03-06T19:14:23.420
CVE-2023-27472	8.2	[{'lang': 'en', 'value': 'quickentity-editor-next is an open source, system local, video game asset editor. In affected versions HTML tags in entity names are not sanitised (XSS vulnerability). Allows arbitrary code execution within the browser sandbox, among other things, simply from loading a file containing a script tag in any entity name. This issue has been patched in version 1.28.1 of the application. Users are advised to upgrade. There are no known workarounds for this vulnerability.'}]	2023-03-06T19:15:10.483	2023-03-06T19:51:54.233
CVE-2023-1211	7.2	[{'lang': 'en', 'value': 'SQL Injection in GitHub repository phpipam/phpipam prior to v1.5.2.'}]	2023-03-07T00:15:09.220	2023-03-07T13:54:09.087
CVE-2023-1238	7.6	[{'lang': 'en', 'value': 'Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6.'}]	2023-03-07T08:15:09.407	2023-03-07T13:54:09.087
CVE-2023-1240	8.0	[{'lang': 'en', 'value': 'Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6.'}]	2023-03-07T08:15:09.580	2023-03-07T13:54:09.087
CVE-2023-1241	8.8	[{'lang': 'en', 'value': 'Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6.'}]	2023-03-07T08:15:09.673	2023-03-07T13:54:09.087
CVE-2023-1242	8.0	[{'lang': 'en', 'value': 'Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6.'}]	2023-03-07T08:15:09.767	2023-03-07T13:54:09.087
CVE-2020-36669	8.8	[{'lang': 'en', 'value': "The JetBackup – WP Backup, Migrate & Restore plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.3.9. This is due to missing nonce validation on the backup_guard_get_import_backup() function. This makes it possible for unauthenticated attackers to upload arbitrary files to the vulnerable site's server via a forged request, granted they can trick a site's administrator into performing an action such as clicking on a link."}]	2023-03-07T14:15:09.357	2023-03-07T14:24:32.077
CVE-2021-44196	7.5	[{'lang': 'en', 'value': 'Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in UBIT Information Technologies Student Information Management System.This issue affects Student Information Management System: before 20211126.'}]	2023-03-07T14:15:09.470	2023-03-07T14:24:32.077
CVE-2021-44197	7.5	[{'lang': 'en', 'value': 'Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in UBIT Information Technologies Student Information Management System.This issue affects Student Information Management System: before 20211126.'}]	2023-03-07T14:15:09.550	2023-03-07T14:24:32.077
CVE-2021-4330	8.8	[{'lang': 'en', 'value': 'The Envato Elements & Download and Template Kit – Import plugins for WordPress are vulnerable to arbitrary file uploads due to insufficient validation of file type upon extracting uploaded Zip files in the installFreeTemplateKit and uploadTemplateKitZipFile functions. This makes it possible for attackers with contributor-lever permissions and above to upload arbitrary files and potentially gain remote code execution in versions up to and including 1.0.13 of Template Kit – Import and versions up to and including 2.0.10 of Envato Elements & Download.'}]	2023-03-07T14:15:09.627	2023-03-07T14:24:32.077
CVE-2021-4331	8.8	[{'lang': 'en', 'value': 'The Plus Addons for Elementor plugin for WordPress is vulnerable to privilege escalation in versions up to, and including 4.1.9 (pro) and 2.0.6 (free). The plugin adds a registration form to the Elementor page builders functionality. As part of the registration form, users can choose which role to set as the default for users upon registration. This field is not hidden for lower-level users so any user with access to the Elementor page builder, such as contributors, can set the default role to administrator. Since contributors can not publish posts, only author+ users can elevate privileges without interaction via a site administrator (to approve a post).'}]	2023-03-07T15:15:10.580	2023-03-07T16:37:02.020
CVE-2023-1253	7.3	[{'lang': 'en', 'value': 'A vulnerability, which was classified as critical, was found in SourceCodester Health Center Patient Record Management System 1.0. This affects an unknown part of the file login.php. The manipulation of the argument username 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-222483.'}]	2023-03-07T15:15:11.067	2023-03-07T16:37:02.020
CVE-2022-39951	7.2	[{'lang': 'en', 'value': "A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWeb version 7.0.0 through 7.0.2, FortiWeb version 6.3.6 through 6.3.20, FortiWeb 6.4 all versions allows attacker to execute unauthorized code or commands via specifically crafted HTTP requests."}]	2023-03-07T17:15:11.877	2023-03-07T17:55:47.627
CVE-2022-39953	7.8	[{'lang': 'en', 'value': 'A improper privilege management in Fortinet FortiNAC version 9.4.0 through 9.4.1, FortiNAC version 9.2.0 through 9.2.6, FortiNAC version 9.1.0 through 9.1.8, FortiNAC all versions 8.8, FortiNAC all versions 8.7, FortiNAC all versions 8.6, FortiNAC all versions 8.5, FortiNAC version 8.3.7 allows attacker to escalation of privilege via specially crafted commands.'}]	2023-03-07T17:15:11.943	2023-03-07T17:55:47.627
CVE-2022-40676	7.5	[{'lang': 'en', 'value': "A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiNAC versions 9.4.0, 9.2.0 through 9.2.5, 9.1.0 through 9.1.8, 8.8.0 through 8.8.11, 8.7.0 through 8.7.6, 8.6.0 through 8.6.5, 8.5.0 through 8.5.4, 8.3.7 allows attacker to execute unauthorized code or commands via specially crafted http requests."}]	2023-03-07T17:15:12.020	2023-03-07T17:55:47.627
CVE-2022-41333	7.5	[{'lang': 'en', 'value': 'An uncontrolled resource consumption vulnerability [CWE-400] in FortiRecorder version 6.4.3 and below, 6.0.11 and below login authentication mechanism may allow an unauthenticated attacker to make the device unavailable via crafted GET requests.'}]	2023-03-07T17:15:12.233	2023-03-07T17:55:47.627
CVE-2022-42476	8.2	[{'lang': 'en', 'value': 'A relative path traversal vulnerability [CWE-23] in Fortinet FortiOS version 7.2.0 through 7.2.2, 7.0.0 through 7.0.8 and before 6.4.11, FortiProxy version 7.2.0 through 7.2.2 and 7.0.0 through 7.0.8 allows privileged VDOM administrators to escalate their privileges to super admin of the box via crafted CLI requests.'}]	2023-03-07T17:15:12.303	2023-03-07T17:55:47.627
CVE-2023-1257	7.6	[{'lang': 'en', 'value': 'An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system.'}]	2023-03-07T17:15:12.527	2023-03-07T17:55:47.627
CVE-2023-25605	7.5	[{'lang': 'en', 'value': 'A improper access control vulnerability in Fortinet FortiSOAR 7.3.0 - 7.3.1 allows an attacker authenticated on the administrative interface to perform unauthorized actions via crafted HTTP requests.'}]	2023-03-07T17:15:12.810	2023-03-07T17:55:47.627
CVE-2023-27475	8.8	[{'lang': 'en', 'value': 'Goutil is a collection of miscellaneous functionality for the go language. In versions prior to 0.6.0 when users use fsutil.Unzip to unzip zip files from a malicious attacker, they may be vulnerable to path traversal. This vulnerability is known as a ZipSlip. This issue has been fixed in version 0.6.0, users are advised to upgrade. There are no known workarounds for this issue.'}]	2023-03-07T18:15:09.170	2023-03-07T18:24:08.837
CVE-2023-27480	7.7	[{'lang': 'en', 'value': 'XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with edit rights on a document can trigger an XAR import on a forged XAR file, leading to the ability to display the content of any file on the XWiki server host. This vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10-rc-1. Users are advised to upgrade. Users unable to upgrade may apply the patch `e3527b98fd` manually.'}]	2023-03-07T19:15:12.663	2023-03-07T20:14:26.217
CVE-2023-27476	8.2	[{'lang': 'en', 'value': "OWSLib is a Python package for client programming with Open Geospatial Consortium (OGC) web service interface standards, and their related content models. OWSLib's XML parser (which supports both `lxml` and `xml.etree`) does not disable entity resolution, and could lead to arbitrary file reads from an attacker-controlled XML payload. This affects all XML parsing in the codebase. This issue has been addressed in version 0.28.1. All users are advised to upgrade. The only known workaround is to patch the library manually. See `GHSA-8h9c-r582-mggc` for details."}]	2023-03-08T00:15:08.997	2023-03-08T13:55:55.097
CVE-2023-0089	8.8	[{'lang': 'en', 'value': "The webutils in Proofpoint Enterprise Protection (PPS/POD) contain a vulnerability that allows an authenticated user to execute remote code through 'eval injection'. This affects all versions 8.20.0 and below."}]	2023-03-08T01:15:10.240	2023-03-08T13:55:55.097
CVE-2023-0090	8.1	[{'lang': 'en', 'value': "The webservices in Proofpoint Enterprise Protection (PPS/POD) contain a vulnerability that allows for an anonymous user to execute remote code through 'eval injection'. Exploitation requires network access to the webservices API, but such access is a non-standard configuration. This affects all versions 8.20.0 and below."}]	2023-03-08T01:15:10.343	2023-03-08T13:55:55.097
CVE-2023-1277	7.8	[{'lang': 'en', 'value': '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	2023-03-08T19:47:01.990
CVE-2023-27486	8.1	[{'lang': 'en', 'value': '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	2023-03-08T19:47:01.990
CVE-2022-4315	7.7	[{'lang': 'en', 'value': 'An issue has been discovered in GitLab DAST analyzer affecting all versions starting from 2.0 before 3.0.55, which sends custom request headers with every request on the authentication page.'}]	2023-03-08T23:15:10.893	2023-03-08T23:15:10.893
CVE-2023-26109	7.3	[{'lang': 'en', 'value': '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	2023-03-09T05:15:56.490
CVE-2023-26110	7.3	[{'lang': 'en', 'value': '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	2023-03-09T05:15:56.947