1. github.com/pariz/gountries :

There are 11,801 CVE records because of GitHub import. (MINOR: there are no problems with the library itself.)

|  |  |
| --- | --- |
| [CVE-2024-24945](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24945) | A stored cross-site scripting (XSS) vulnerability in Travel Journal Using PHP and MySQL with Source Code v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Share Your Moments parameter at /travel-journal/write-journal.php. |
| [CVE-2024-24760](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24760) | This vulnerability potentially allows attackers on the same subnet to connect to exposed ports of a Docker container, even when the port is bound to 127.0.0.1. The vulnerability has been addressed by implementing additional iptables/nftables rules |
| [CVE-2024-24757](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24757) | open-irs is an issue response robot that reponds to issues in the installed repository. The `.env` file was accidentally uploaded when working with git actions. This problem is fixed in 1.0.1. Discontinuing all sensitive keys and turning into secrets. |
| [CVE-2024-24756](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24756) | Crafatar serves Minecraft avatars based on the skin for use in external applications. Files outside of the `lib/public/` directory can be requested from the server. |
| [CVE-2024-24755](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24755) | discourse-group-membership-ip-block is a discourse plugin that adds support for adding users to groups based on their IP address. discourse-group-membership-ip-block was sending all group custom fields to the client, including group custom fields from other plugins which may expect their custom fields to remain secret. |
| [CVE-2024-24754](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24754) | Bref enable serverless PHP on AWS Lambda. When Bref is used with the Event-Driven Function runtime and the handler is a `RequestHandlerInterface`, then the Lambda event is converted to a PSR7 object. |
| [CVE-2024-24753](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24753) | Bref enable serverless PHP on AWS Lambda. When Bref is used in combination with an API Gateway with the v2 format, it does not handle multiple values headers. If PHP generates a response with two headers having the same key but different values only the latest one is kept. |
| [CVE-2024-24752](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24752) | Bref enable serverless PHP on AWS Lambda. When Bref is used with the Event-Driven Function runtime and the handler is a `RequestHandlerInterface`, then the Lambda event is converted to a PSR7 object. During the conversion process, if the request is a MultiPart, each part is parsed and for each which contains a file, it is extracted and saved in `/tmp` with a random filename starting with `bref\_upload\_`. |

1. Go.opentelemetry.io/otel/trace

There are **1** CVE Records (MINOR issue fixed from version 0.46.0) :

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  | | --- | --- | | [CVE-2023-47108](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-47108) |  | | OpenTelemetry-Go Contrib is a collection of third-party packages for OpenTelemetry-Go. Prior to version 0.46.0, the grpc Unary Server Interceptor out of the box adds labels `net.peer.sock.addr` and `net.peer.sock.port` that have unbound cardinality. It leads to the server's potential memory exhaustion when many malicious requests are sent. An attacker can easily flood the peer address and port for requests. Version 0.46.0 contains a fix for this issue. As a workaround to stop being affected, a view removing the attributes can be used. The other possibility is to disable grpc metrics instrumentation by passing `otelgrpc.WithMeterProvider` option with `noop.NewMeterProvider`. |

1. github.com/sony/gobreaker

There are **11851** CVE Records because of GitHub import. (MINOR: there are no problems with the library itself.)

|  |  |
| --- | --- |
| [CVE-2024-24747](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24747) | MinIO is a High Performance Object Storage. When someone creates an access key, it inherits the permissions of the parent key. Not only for `s3:\*` actions, but also `admin:\*` actions. Which means unless somewhere above in the access-key hierarchy, the `admin` rights are denied, access keys will be able to simply override their own `s3` permissions to something more permissive. The vulnerability is fixed in RELEASE.2024-01-31T20-20-33Z. |
| [CVE-2024-24579](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24579) | stereoscope is a go library for processing container images and simulating a squash filesystem. Prior to version 0.0.1, it is possible to craft an OCI tar archive that, when stereoscope attempts to unarchive the contents, will result in writing to paths outside of the unarchive temporary directory. |
| [CVE-2024-24573](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24573) | facileManager is a modular suite of web apps built with the sysadmin in mind. In versions 4.5.0 and earlier, when a user updates their profile, a POST request containing user information is sent to the endpoint server/fm-modules/facileManager/ajax/processPost.php. It was found that non-admins can arbitrarily set their permissions and grant their non-admin accounts with super user privileges. |
| [CVE-2024-24572](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24572) | facileManager is a modular suite of web apps built with the sysadmin in mind. In versions 4.5.0 and earlier, the $\_REQUEST global array was unsafely called inside an extract() function in admin-logs.php. The PHP file fm-init.php prevents arbitrary manipulation of $\_SESSION via the GET/POST parameters. However, it does not prevent manipulation of any other sensitive variables such as $search\_sql. |
| [CVE-2024-24571](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24571) | facileManager is a modular suite of web apps built with the sysadmin in mind. For the facileManager web application versions 4.5.0 and earlier, we have found that XSS was present in almost all of the input fields as there is insufficient input validation. |
| [CVE-2024-24570](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24570) | Statamic is a Laravel and Git powered CMS. HTML files crafted to look like jpg files are able to be uploaded, allowing for XSS. This affects the front-end forms with asset fields without any mime type validation, asset fields in the control panel, and asset browser in the control panel. |
| [CVE-2024-24569](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24569) | The Pixee Java Code Security Toolkit is a set of security APIs meant to help secure Java code. `ZipSecurity#isBelowCurrentDirectory` is vulnerable to a partial-path traversal bypass. To be vulnerable to the bypass, the application must use toolkit version <=1.1.1, use ZipSecurity as a guard against path traversal, and have an exploit path. |
| [CVE-2024-24567](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24567) | Vyper is a pythonic Smart Contract Language for the ethereum virtual machine. Vyper compiler allows passing a value in builtin raw\_call even if the call is a delegatecall or a staticcall. But in the context of delegatecall and staticcall the handling of value is not possible due to the semantics of the respective opcodes, and vyper will silently ignore the value= argument. |

1. Github.com/sirupsen/logrus

There are **11851** CVE Records because of GitHub import. (MINOR: there are no problems with the library itself.)

|  |  |
| --- | --- |
| [CVE-2024-24558](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24558) | TanStack Query supplies asynchronous state management, server-state utilities and data fetching for the web. The `@tanstack/react-query-next-experimental` NPM package is vulnerable to a cross-site scripting vulnerability. To exploit this, an attacker would need to either inject malicious input or arrange to have malicious input be returned from an endpoint. To fix this issue, please update to version 5.18.0 or later. |
| [CVE-2024-24557](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24557) | Moby is an open-source project created by Docker to enable software containerization. The classic builder cache system is prone to cache poisoning if the image is built FROM scratch. Also, changes to some instructions (most important being HEALTHCHECK and ONBUILD) would not cause a cache miss. |
| |  |  | | --- | --- | | [CVE-2024-24556](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24556) |  | | urql is a GraphQL client that exposes a set of helpers for several frameworks. The `@urql/next` package is vulnerable to XSS. To exploit this an attacker would need to ensure that the response returns `html` tags and that the web-application is using streamed responses (non-RSC). This vulnerability is due to improper escaping of html-like characters in the response-stream. To fix this vulnerability upgrade to version 1.1.1 |
| [CVE-2024-23941](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23941) | Cross-site scripting vulnerability exists in Group Office prior to v6.6.182, prior to v6.7.64 and prior to v6.8.31, which may allow a remote authenticated attacker to execute an arbitrary script on the web browser of the user who is logging in to the product. |
| [CVE-2024-23841](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23841) | apollo-client-nextjs is the Apollo Client support for the Next.js App Router. The @apollo/experimental-apollo-client-nextjs NPM package is vulnerable to a cross-site scripting vulnerability. To exploit this vulnerability, an attacker would need to either inject malicious input (e.g. by redirecting a user to a specifically-crafted link) or arrange to have malicious input be returned by a GraphQL server (e.g. by persisting it in a database). To fix this issue, please update to version 0.7.0 or later. |
| [CVE-2024-23840](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23840) | GoReleaser builds Go binaries for several platforms, creates a GitHub release and then pushes a Homebrew formula to a tap repository. `goreleaser release --debug` log shows secret values used in the in the custom publisher. This vulnerability is fixed in 1.24.0. |
| [CVE-2024-23838](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23838) | TrueLayer.NET is the .Net client for TrueLayer. The vulnerability could potentially allow a malicious actor to gain control over the destination URL of the HttpClient used in the API classes. For applications using the SDK, requests to unexpected resources on local networks or to the internet could be made which could lead to information disclosure. |
| [CVE-2024-23834](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23834) | Discourse is an open-source discussion platform. Improperly sanitized user input could lead to an XSS vulnerability in some situations. This vulnerability only affects Discourse instances which have disabled the default Content Security Policy. The vulnerability is patched in 3.1.5 and 3.2.0.beta5. As a workaround, ensure Content Security Policy is enabled and does not include `unsafe-inline`. |

1. go.mongodb.org/mongo-driver/bson

There are **20** CVE Records (MODERATE)

|  |  |
| --- | --- |
| [CVE-2019-17426](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17426) | Automattic Mongoose through 5.7.4 allows attackers to bypass access control (in some applications) because any query object with a \_bsontype attribute is ignored. For example, adding "\_bsontype":"a" can sometimes interfere with a query filter. NOTE: this CVE is about Mongoose's failure to work around this \_bsontype special case that exists in older versions of the bson parser (aka the mongodb/js-bson project). |
| [CVE-2019-11484](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11484) | Kevin Backhouse discovered an integer overflow in bson\_ensure\_space, as used in whoopsie. |
| [CVE-2018-16790](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16790) | \_bson\_iter\_next\_internal in bson-iter.c in libbson 1.12.0, as used in MongoDB mongo-c-driver and other products, has a heap-based buffer over-read via a crafted bson buffer. |
| [CVE-2018-13863](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13863) | The MongoDB bson JavaScript module (also known as js-bson) versions 0.5.0 to 1.0.x before 1.0.5 is vulnerable to a Regular Expression Denial of Service (ReDoS) in lib/bson/decimal128.js. The flaw is triggered when the Decimal128.fromString() function is called to parse a long untrusted string. |
| [CVE-2017-14227](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14227) | In MongoDB libbson 1.7.0, the bson\_iter\_codewscope function in bson-iter.c miscalculates a bson\_utf8\_validate length argument, which allows remote attackers to cause a denial of service (heap-based buffer over-read in the bson\_utf8\_validate function in bson-utf8.c), as demonstrated by bson-to-json.c. |
| [CVE-2015-4412](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4412) | BSON injection vulnerability in the legal? function in BSON (bson-ruby) gem before 3.0.4 for Ruby allows remote attackers to cause a denial of service (resource consumption) or inject arbitrary data via a crafted string. |
| [CVE-2015-4411](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4411) | The Moped::BSON::ObjecId.legal? method in mongodb/bson-ruby before 3.0.4 as used in rubygem-moped allows remote attackers to cause a denial of service (worker resource consumption) via a crafted string. NOTE: This issue is due to an incomplete fix to CVE-2015-4410. |
| [CVE-2015-4410](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4410) | The Moped::BSON::ObjecId.legal? method in rubygem-moped before commit dd5a7c14b5d2e466f7875d079af71ad19774609b allows remote attackers to cause a denial of service (worker resource consumption) or perform a cross-site scripting (XSS) attack via a crafted string. |

|  |  |
| --- | --- |
| [CVE-2023-36475](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36475) | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 5.5.2 and 6.2.1, an attacker can use a prototype pollution sink to trigger a remote code execution through the MongoDB BSON parser. A patch is available in versions 5.5.2 and 6.2.1. |
| [CVE-2023-0437](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0437) | When calling bson\_utf8\_validate on some inputs a loop with an exit condition that cannot be reached may occur, i.e. an infinite loop. This issue affects All MongoDB C Driver versions prior to versions 1.25.0. |
| [CVE-2022-39396](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39396) | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Versions prior to 4.10.18, and prior to 5.3.1 on the 5.X branch, are vulnerable to Remote Code Execution via prototype pollution. An attacker can use this prototype pollution sink to trigger a remote code execution through the MongoDB BSON parser. This issue is patched in version 5.3.1 and in 4.10.18. There are no known workarounds. |
| [CVE-2021-20329](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20329) | Specific cstrings input may not be properly validated in the MongoDB Go Driver when marshalling Go objects into BSON. A malicious user could use a Go object with specific string to potentially inject additional fields into marshalled documents. This issue affects all MongoDB GO Drivers prior to and including 1.5.0. |
| [CVE-2020-7610](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7610) | All versions of bson before 1.1.4 are vulnerable to Deserialization of Untrusted Data. The package will ignore an unknown value for an object's \_bsotype, leading to cases where an object is serialized as a document rather than the intended BSON type. |
| [CVE-2020-12135](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12135) | bson before 0.8 incorrectly uses int rather than size\_t for many variables, parameters, and return values. In particular, the bson\_ensure\_space() parameter bytesNeeded could have an integer overflow via properly constructed bson input. |
| [CVE-2019-2391](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2391) | Incorrect parsing of certain JSON input may result in js-bson not correctly serializing BSON. This may cause unexpected application behaviour including data disclosure. This issue affects: MongoDB Inc. js-bson library version 1.1.3 and prior to. |
| [CVE-2019-19729](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19729) | An issue was discovered in the BSON ObjectID (aka bson-objectid) package 1.3.0 for Node.js. ObjectID() allows an attacker to generate a malformed objectid by inserting an additional property to the user-input, because bson-objectid will return early if it detects \_bsontype==ObjectID in the user-input object. As a result, objects in arbitrary forms can bypass formatting if they have a valid bsontype. |

6. github.com/go-redis/redis

There are **53** CVE Records (MODERATE)

|  |  |
| --- | --- |
| [CVE-2023-50727](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-50727) | Resque is a Redis-backed Ruby library for creating background jobs, placing them on multiple queues, and processing them later. Reflected XSS issue occurs when /queues is appended with /"><svg%20onload=alert(domain)>. This issue has been patched in version 2.6.0. |
| [CVE-2023-50725](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-50725) | Resque is a Redis-backed Ruby library for creating background jobs, placing them on multiple queues, and processing them later. The following paths in resque-web have been found to be vulnerable to reflected XSS: "/failed/?class=<script>alert(document.cookie)</script>" and "/queues/><img src=a onerror=alert(document.cookie)>". This issue has been patched in version 2.2.1. |
| [CVE-2023-50724](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-50724) | Resque (pronounced like "rescue") is a Redis-backed library for creating background jobs, placing those jobs on multiple queues, and processing them later. resque-web in resque versions before 2.1.0 are vulnerable to reflected XSS through the current\_queue parameter in the path of the queues endpoint. This issue has been patched in version 2.1.0. |
| [CVE-2023-47120](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-47120) | Discourse is an open source platform for community discussion. In versions 3.1.0 through 3.1.2 of the `stable` branch and versions 3.1.0,beta6 through 3.2.0.beta2 of the `beta` and `tests-passed` branches, Redis memory can be depleted by crafting a site with an abnormally long favicon URL and drafting multiple posts which Onebox it. The issue is patched in version 3.1.3 of the `stable` branch and version 3.2.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds. |
| [CVE-2023-45148](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-45148) | Nextcloud is an open source home cloud server. When Memcached is used as `memcache.distributed` the rate limiting in Nextcloud Server could be reset unexpectedly resetting the rate count earlier than intended. Users are advised to upgrade to versions 25.0.11, 26.0.6 or 27.1.0. Users unable to upgrade should change their config setting `memcache.distributed` to `\OC\Memcache\Redis` and install Redis instead of Memcached. |
| [CVE-2023-45145](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-45145) | Redis is an in-memory database that persists on disk. On startup, Redis begins listening on a Unix socket before adjusting its permissions to the user-provided configuration. If a permissive umask(2) is used, this creates a race condition that enables, during a short period of time, another process to establish an otherwise unauthorized connection. |
| [CVE-2023-42809](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42809) | Redisson is a Java Redis client that uses the Netty framework. Prior to version 3.22.0, some of the messages received from the Redis server contain Java objects that the client deserializes without further validation. Attackers that manage to trick clients into communicating with a malicious server can include especially crafted objects in its responses that, once deserialized by the client, force it to execute arbitrary code. |
| [CVE-2023-41056](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41056) | Redis is an in-memory database that persists on disk. Redis incorrectly handles resizing of memory buffers which can result in integer overflow that leads to heap overflow and potential remote code execution. This issue has been patched in version 7.0.15 and 7.2.4. |

|  |  |
| --- | --- |
| [CVE-2023-41053](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41053) | Redis is an in-memory database that persists on disk. Redis does not correctly identify keys accessed by `SORT\_RO` and as a result may grant users executing this command access to keys that are not explicitly authorized by the ACL configuration. The problem exists in Redis 7.0 or newer and has been fixed in Redis 7.0.13 and 7.2.1. Users are advised to upgrade. There are no known workarounds for this vulnerability. |
| [CVE-2023-36824](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36824) | Redis is an in-memory database that persists on disk. In Redit 7.0 prior to 7.0.12, extracting key names from a command and a list of arguments may, in some cases, trigger a heap overflow and result in reading random heap memory, heap corruption and potentially remote code execution. |
| [CVE-2023-28859](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28859) | redis-py before 4.4.4 and 4.5.x before 4.5.4 leaves a connection open after canceling an async Redis command at an inopportune time, and can send response data to the client of an unrelated request. (This could, for example, happen for a non-pipeline operation.) NOTE: the solutions for CVE-2023-28859 address data leakage across AsyncIO connections in general. |
| [CVE-2023-28858](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28858) | redis-py before 4.5.3 leaves a connection open after canceling an async Redis command at an inopportune time, and can send response data to the client of an unrelated request in an off-by-one manner. NOTE: this CVE Record was initially created in response to reports about ChatGPT, and 4.3.6, 4.4.3, and 4.5.3 were released (changing the behavior for pipeline operations); however, please see CVE-2023-28859 about addressing data leakage across AsyncIO connections in general. |
| [CVE-2023-28856](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28856) | Redis is an open source, in-memory database that persists on disk. Authenticated users can use the `HINCRBYFLOAT` command to create an invalid hash field that will crash Redis on access in affected versions. This issue has been addressed in in versions 7.0.11, 6.2.12, and 6.0.19. Users are advised to upgrade. There are no known workarounds for this issue. |
| [CVE-2023-28425](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28425) | Redis is an in-memory database that persists on disk. Starting in version 7.0.8 and prior to version 7.0.10, authenticated users can use the MSETNX command to trigger a runtime assertion and termination of the Redis server process. The problem is fixed in Redis version 7.0.10. |
| [CVE-2023-25155](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25155) | Redis is an in-memory database that persists on disk. Authenticated users issuing specially crafted `SRANDMEMBER`, `ZRANDMEMBER`, and `HRANDFIELD` commands can trigger an integer overflow, resulting in a runtime assertion and termination of the Redis server process. This problem affects all Redis versions. Patches were released in Redis version(s) 6.0.18, 6.2.11 and 7.0.9. |
| [CVE-2023-22458](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22458) | Redis is an in-memory database that persists on disk. Authenticated users can issue a `HRANDFIELD` or `ZRANDMEMBER` command with specially crafted arguments to trigger a denial-of-service by crashing Redis with an assertion failure. This problem affects Redis versions 6.2 or newer up to but not including 6.2.9 as well as versions 7.0 up to but not including 7.0.8. Users are advised to upgrade. There are no known workarounds for this vulnerability. |

1. Github.com/colinmarc/hdfs/v2

There are **53** CVE Records (MODERATE)

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  | | --- | --- | | [CVE-2024-24753](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24753) |  | | Bref enable serverless PHP on AWS Lambda. When Bref is used in combination with an API Gateway with the v2 format, it does not handle multiple values headers. If PHP generates a response with two headers having the same key but different values only the latest one is kept. If an application relies on multiple headers with the same key being set for security reasons, then Bref would lower the application security. For example, if an application sets multiple `Content-Security-Policy` headers, then Bref would just reflect the latest one. This vulnerability is patched in 2.1.13. |
| [CVE-2024-0717](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-0717) | A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. |
| [CVE-2023-7208](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-7208) | A vulnerability classified as critical was found in Totolink X2000R\_V2 2.0.0-B20230727.10434. This vulnerability affects the function formTmultiAP of the file /bin/boa. The manipulation leads to buffer overflow. VDB-249742 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. |
| [CVE-2023-5020](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5020) | A vulnerability, which was classified as critical, has been found in 07FLY CRM V2. This issue affects some unknown processing of the file /index.php/sysmanage/Login/login\_auth/ of the component Administrator Login Page. The manipulation of the argument account leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-239861 was assigned to this vulnerability. |
| [CVE-2023-49297](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-49297) | PyDrive2 is a wrapper library of google-api-python-client that simplifies many common Google Drive API V2 tasks. Unsafe YAML deserilization will result in arbitrary code execution. A maliciously crafted YAML file can cause arbitrary code execution if PyDrive2 is run in the same directory as it, or if it is loaded in via `LoadSettingsFile`. This is a deserilization attack that will affect any user who initializes GoogleAuth from this package while a malicious yaml file is present in the same directory. This vulnerability does not require the file to be directly loaded through the code, only present. This issue has been addressed in commit `c57355dc` which is included in release version `1.16.2`. Users are advised to upgrade. There are no known workarounds for this vulnerability. |
| [CVE-2023-46139](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46139) | KernelSU is a Kernel based root solution for Android. Starting in version 0.6.1 and prior to version 0.7.0, if a KernelSU installed device is infected with a malware whose app signing block specially constructed, it can take over root privileges on the device. The vulnerable verification logic actually obtains the signature of the last block with an id of `0x7109871a`, while the verification logic during Android installation is to obtain the first one. In addition to the actual signature upgrade that has been fixed (KSU thought it was V2 but was actually V3), there is also the problem of actual signature downgrading (KSU thought it was V2 but was actually V1). Find a condition in the signature verification logic that will cause the signature not to be found error, and KernelSU does not implement the same conditions, so KSU thinks there is a V2 signature, but the APK signature verification actually uses the V1 signature. This issue is fixed in version 0.7.0. As workarounds, keep the KernelSU manager installed and avoid installing unknown apps. |
| |  |  | | --- | --- | | [CVE-2023-45142](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-45142) |  | | OpenTelemetry-Go Contrib is a collection of third-party packages for OpenTelemetry-Go. A handler wrapper out of the box adds labels `http.user\_agent` and `http.method` that have unbound cardinality. It leads to the server's potential memory exhaustion when many malicious requests are sent to it. HTTP header User-Agent or HTTP method for requests can be easily set by an attacker to be random and long. The library internally uses `httpconv.ServerRequest` that records every value for HTTP `method` and `User-Agent`. In order to be affected, a program has to use the `otelhttp.NewHandler` wrapper and not filter any unknown HTTP methods or User agents on the level of CDN, LB, previous middleware, etc. Version 0.44.0 fixed this issue when the values collected for attribute `http.request.method` were changed to be restricted to a set of well-known values and other high cardinality attributes were removed. As a workaround to stop being affected, `otelhttp.WithFilter()` can be used, but it requires manual careful configuration to not log certain requests entirely. For convenience and safe usage of this library, it should by default mark with the label `unknown` non-standard HTTP methods and User agents to show that such requests were made but do not increase cardinality. In case someone wants to stay with the current behavior, library API should allow to enable it. |
| [CVE-2023-43803](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-43803) | Arduino Create Agent is a package to help manage Arduino development. This vulnerability affects the endpoint `/v2/pkgs/tools/installed` and the way it handles plugin names supplied as user input. A user who has the ability to perform HTTP requests to the localhost interface, or is able to bypass the CORS configuration, can delete arbitrary files or folders belonging to the user that runs the Arduino Create Agent via a crafted HTTP POST request. This issue has been addressed in version `1.3.3`. Users are advised to upgrade. There are no known workarounds for this vulnerability. |

1. metrics\_query/domain

There are **1941** CVE Records (MINOR)

|  |  |
| --- | --- |
| [CVE-2024-22424](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-22424) | Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. The Argo CD API prior to versions 2.10-rc2, 2.9.4, 2.8.8, and 2.7.15 are vulnerable to a cross-server request forgery (CSRF) attack when the attacker has the ability to write HTML to a page on the same parent domain as Argo CD. A CSRF attack works by tricking an authenticated Argo CD user into loading a web page which contains code to call Argo CD API endpoints on the victim&#8217;s behalf. For example, an attacker could send an Argo CD user a link to a page which looks harmless but in the background calls an Argo CD API endpoint to create an application running malicious code. |
| [CVE-2024-22417](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-22417) | Whoogle Search is a self-hosted metasearch engine. In versions 0.8.3 and prior, the `element` method in `app/routes.py` does not validate the user-controlled `src\_type` and `element\_url` variables and passes them to the `send` method which sends a `GET` request on lines 339-343 in `requests.py`. The returned contents of the URL are then passed to and reflected back to the user in the `send\_file` function on line 484, together with the user-controlled `src\_type`, which allows the attacker to control the HTTP response content type leading to a cross-site scripting vulnerability. An attacker could craft a special URL to point to a malicious website and send the link to a victim. The fact that the link would contain a trusted domain (e.g. from one of public Whoogle instances) could be used to trick the user into clicking the link. The malicious website could, for example, be a copy of a real website, meant to steal a person&#8217;s credentials to the website, or trick that person in another way. Version 0.8.4 contains a patch for this issue. |
| [CVE-2024-21641](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-21641) | Flarum is open source discussion platform software. Prior to version 1.8.5, the Flarum `/logout` route includes a redirect parameter that allows any third party to redirect users from a (trusted) domain of the Flarum installation to redirect to any link. For logged-in users, the logout must be confirmed. Guests are immediately redirected. This could be used by spammers to redirect to a web address using a trusted domain of a running Flarum installation. The vulnerability has been fixed and published as flarum/core v1.8.5. As a workaround, some extensions modifying the logout route can remedy this issue if their implementation is safe. |
| [CVE-2024-0805](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-0805) | Inappropriate implementation in Downloads in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to perform domain spoofing via a crafted domain name. (Chromium security severity: Medium) |
| [CVE-2023-7227](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-7227) | SystemK NVR 504/508/516 versions 2.3.5SK.30084998 and prior are vulnerable to a command injection vulnerability in the dynamic domain name system (DDNS) settings that could allow an attacker to execute arbitrary commands with root privileges. |
| [CVE-2023-7025](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-7025) | A vulnerability was found in KylinSoft hedron-domain-hook up to 3.8.0.12-0k0.5. It has been declared as critical. This vulnerability affects the function init\_kcm of the component DBus Handler. The manipulation leads to improper access controls. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. VDB-248578 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. |
| [CVE-2023-7008](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-7008) | A vulnerability was found in systemd-resolved. This issue may allow systemd-resolved to accept records of DNSSEC-signed domains even when they have no signature, allowing man-in-the-middles (or the upstream DNS resolver) to manipulate records. |
| [CVE-2023-5986](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5986) | A CWE-601 URL Redirection to Untrusted Site vulnerability exists that could cause an openredirect vulnerability leading to a cross site scripting attack. By providing a URL-encoded input attackers can cause the software&#8217;s web application to redirect to the chosen domain after a successful login is performed. |

1. example/metrics\_events

There are **1183** CVE Records (MINOR)

|  |  |
| --- | --- |
| [CVE-2023-4502](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4502) | The Translate WordPress with GTranslate WordPress plugin before 3.0.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered\_html capability is disallowed (for example in multisite setup). This vulnerability affects multiple parameters. |
| [CVE-2023-44216](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44216) | PVRIC (PowerVR Image Compression) on Imagination 2018 and later GPU devices offers software-transparent compression that enables cross-origin pixel-stealing attacks against feTurbulence and feBlend in the SVG Filter specification, aka a GPU.zip issue. For example, attackers can sometimes accurately determine text contained on a web page from one origin if they control a resource from a different origin. |
| [CVE-2023-4421](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4421) | The NSS code used for checking PKCS#1 v1.5 was leaking information useful in mounting Bleichenbacher-like attacks. Both the overall correctness of the padding as well as the length of the encrypted message was leaking through timing side-channel. By sending large number of attacker-selected ciphertexts, the attacker would be able to decrypt a previously intercepted PKCS#1 v1.5 ciphertext (for example, to decrypt a TLS session that used RSA key exchange), or forge a signature using the victim's key. The issue was fixed by implementing the implicit rejection algorithm, in which the NSS returns a deterministic random message in case invalid padding is detected, as proposed in the Marvin Attack paper. This vulnerability affects NSS < 3.61. |
| [CVE-2023-4390](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4390) | The Popup box WordPress plugin before 3.7.2 does not sanitize and escape some Popup fields, which could allow high-privilege users such as an administrator to inject arbitrary web scripts even when the unfiltered\_html capability is disallowed (for example in a multisite setup). |
| [CVE-2023-4388](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4388) | The EventON WordPress plugin before 2.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered\_html capability is disallowed (for example in multisite setup) |
| [CVE-2023-4376](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4376) | The Serial Codes Generator and Validator with WooCommerce Support WordPress plugin before 2.4.15 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered\_html capability is disallowed (for example in multisite setup) |
| [CVE-2023-4298](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4298) | The 123.chat WordPress plugin before 1.3.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered\_html capability is disallowed (for example in multisite setup) |
| [CVE-2023-4254](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4254) | The AI ChatBot WordPress plugin before 4.7.8 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered\_html capability is disallowed (for example in multisite setup) |

9. github.com/gofrs/uuid

There are **16** CVE Records (MODERATE)

|  |  |
| --- | --- |
| [CVE-2024-23329](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23329) | changedetection.io is an open source tool designed to monitor websites for content changes. In affected versions the API endpoint `/api/v1/watch/<uuid>/history` can be accessed by any unauthorized user. As a result any unauthorized user can check one's watch history. However, because unauthorized party first needs to know a watch UUID, and the watch history endpoint itself returns only paths to the snapshot on the server, an impact on users' data privacy is minimal. This issue has been addressed in version 0.45.13. Users are advised to upgrade. There are no known workarounds for this vulnerability. |
| [CVE-2024-22194](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-22194) | cdo-local-uuid project provides a specialized UUID-generating function that can, on user request, cause a program to generate deterministic UUIDs. An information leakage vulnerability is present in `cdo-local-uuid` at version `0.4.0`, and in `case-utils` in unpatched versions (matching the pattern `0.x.0`) at and since `0.5.0`, before `0.15.0`. The vulnerability stems from a Python function, `cdo\_local\_uuid.local\_uuid()`, and its original implementation `case\_utils.local\_uuid()`. |
| [CVE-2023-3485](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-3485) | Insecure defaults in open-source Temporal Server before version 1.20 on all platforms allows an attacker to craft a task token with access to a namespace other than the one specified in the request. Creation of this task token must be done outside of the normal Temporal server flow. It requires the namespace UUID and information from the workflow history for the target namespace. Under these conditions, it is possible to interfere with pending tasks in other namespaces, such as marking a task failed or completed. If a task is targeted for completion by the attacker, the targeted namespace must also be using the same data converter configuration as the initial, valid, namespace for the task completion payload to be decoded by workers in the target namespace. |
| |  |  | | --- | --- | | [CVE-2023-28108](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28108) |  | | 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. |
| [CVE-2023-1065](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-1065) | This vulnerability in the Snyk Kubernetes Monitor can result in irrelevant data being posted to a Snyk Organization, which could in turn obfuscate other, relevant, security issues. It does not expose the user of the integration to any direct security risk and no user data can be leaked. To exploit the vulnerability the attacker does not need to be authenticated to Snyk but does need to know the target's Integration ID (which may or may not be the same as the Organization ID, although this is an unpredictable UUID in either case). |
| [CVE-2022-24781](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24781) | Geon is a board game based on solving questions about the Pythagorean Theorem. Malicious users can obtain the uuid from other users, spoof that uuid through the browser console and become co-owners of the target session. This issue is patched in version 1.1.0. No known workaround exists. |
| [CVE-2021-3628](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3628) | OpenKM Community Edition in its 6.3.10 version is vulnerable to authenticated Cross-site scripting (XSS). A remote attacker could exploit this vulnerability by injecting arbitrary code via de uuid parameter. |
| [CVE-2012-5563](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5563) | OpenStack Keystone, as used in OpenStack Folsom 2012.2, does not properly implement token expiration, which allows remote authenticated users to bypass intended authorization restrictions by creating new tokens through token chaining. NOTE: this issue exists because of a CVE-2012-3426 regression. |

10. github.com/EventStore/EventStore-Client-Go/esdb

There are 11,801 CVE records because of GitHub import. (MINOR: there are no problems with the library itself.)

|  |  |
| --- | --- |
| [CVE-2024-22049](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-22049) | httparty before 0.21.0 is vulnerable to an assumed-immutable web parameter vulnerability. A remote and unauthenticated attacker can provide a crafted filename parameter during multipart/form-data uploads which could result in attacker controlled filenames being written |
| [CVE-2024-22048](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-22048) | govuk\_tech\_docs versions from 2.0.2 to before 3.3.1 are vulnerable to a cross-site scripting vulnerability. Malicious JavaScript may be executed in the user's browser if a malicious search result is displayed on the search page. |
| [CVE-2024-22047](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-22047) | A race condition exists in Audited 4.0.0 to 5.3.3 that can result in an authenticated user to cause audit log entries to be attributed to another user. |
| [CVE-2024-21911](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-21911) | TinyMCE versions before 5.6.0 are affected by a stored cross-site scripting vulnerability. An unauthenticated and remote attacker could insert crafted HTML into the editor resulting in arbitrary JavaScript execution in another user's browser. |
| [CVE-2024-21910](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-21910) | TinyMCE versions before 5.10.0 are affected by a cross-site scripting vulnerability. A remote and unauthenticated attacker could introduce crafted image or link URLs that would result in the execution of arbitrary JavaScript in an editing user's browser. |

11. github.com/neo4j/neo4j-go-driver/v5/neo4j

There are **11** CVE Records

|  |  |
| --- | --- |
| [CVE-2024-23638](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23638) | Squid is a caching proxy for the Web. Due to an expired pointer reference bug, Squid prior to version 6.6 is vulnerable to a Denial of Service attack against Cache Manager error responses. This problem allows a trusted client to perform Denial of Service when generating error pages for Client Manager reports. Squid older than 5.0.5 have not been tested and should be assumed to be vulnerable. All Squid-5.x up to and including 5.9 are vulnerable. All Squid-6.x up to and including 6.5 are vulnerable. This bug is fixed by Squid version 6.6. In addition, patches addressing this problem for the stable releases can be found in Squid's patch archives. As a workaround, prevent access to Cache Manager using Squid's main access control: `http\_access deny manager`. |
| [CVE-2023-50269](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-50269) | Squid is a caching proxy for the Web. Due to an Uncontrolled Recursion bug in versions 2.6 through 2.7.STABLE9, versions 3.1 through 5.9, and versions 6.0.1 through 6.5, Squid may be vulnerable to a Denial of Service attack against HTTP Request parsing. This problem allows a remote client to perform Denial of Service attack by sending a large X-Forwarded-For header when the follow\_x\_forwarded\_for feature is configured. This bug is fixed by Squid version 6.6. In addition, patches addressing this problem for the stable releases can be found in Squid's patch archives. |
| [CVE-2023-49569](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-49569) | A path traversal vulnerability was discovered in go-git versions prior to v5.11. This vulnerability allows an attacker to create and amend files across the filesystem. In the worse case scenario, remote code execution could be achieved. Applications are only affected if they are using the ChrootOS https://pkg.go.dev/github.com/go-git/go-billy/v5/osfs#ChrootOS , which is the default when using "Plain" versions of Open and Clone funcs (e.g. PlainClone). Applications using BoundOS https://pkg.go.dev/github.com/go-git/go-billy/v5/osfs#BoundOS or in-memory filesystems are not affected by this issue. This is a go-git implementation issue and does not affect the upstream git cli. |
| [CVE-2023-49285](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-49285) | Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. Due to a Buffer Overread bug Squid is vulnerable to a Denial of Service attack against Squid HTTP Message processing. This bug is fixed by Squid version 6.5. Users are advised to upgrade. There are no known workarounds for this vulnerability. |
| [CVE-2023-46724](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46724) | Squid is a caching proxy for the Web. Due to an Improper Validation of Specified Index bug, Squid versions 3.3.0.1 through 5.9 and 6.0 prior to 6.4 compiled using `--with-openssl` are vulnerable to a Denial of Service attack against SSL Certificate validation. This problem allows a remote server to perform Denial of Service against Squid Proxy by initiating a TLS Handshake with a specially crafted SSL Certificate in a server certificate chain. This attack is limited to HTTPS and SSL-Bump. This bug is fixed in Squid version 6.4. In addition, patches addressing this problem for the stable releases can be found in Squid's patch archives. Those who you use a prepackaged version of Squid should refer to the package vendor for availability information on updated packages. |
| [CVE-2022-41318](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41318) | A buffer over-read was discovered in libntlmauth in Squid 2.5 through 5.6. Due to incorrect integer-overflow protection, the SSPI and SMB authentication helpers are vulnerable to reading unintended memory locations. In some configurations, cleartext credentials from these locations are sent to a client. This is fixed in 5.7. |
| [CVE-2022-41317](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41317) | An issue was discovered in Squid 4.9 through 4.17 and 5.0.6 through 5.6. Due to inconsistent handling of internal URIs, there can be Exposure of Sensitive Information about clients using the proxy via an HTTPS request to an internal cache manager URL. This is fixed in 5.7. |
| [CVE-2021-37704](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37704) | PhpFastCache is a high-performance backend cache system (packagist package phpfastcache/phpfastcache). In versions before 6.1.5, 7.1.2, and 8.0.7 the `phpinfo()` can be exposed if the `/vendor` is not protected from public access. This is a rare situation today since the vendor directory is often located outside the web directory or protected via server rule (.htaccess, etc). Only the v6, v7 and v8 will be patched respectively in 8.0.7, 7.1.2, 6.1.5. Older versions such as v5, v4 are not longer supported and will \*\*NOT\*\* be patched. As a workaround, protect the `/vendor` directory from public access. |