Reducing Ratio of Reserved But Public CVEs

Shelby Cunningham (she/her), GitHub
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserved but Public (RBP)</td>
<td>A CVE ID in the &quot;Reserved&quot; state that is referenced in one or more public sources but for which a CVE Record has not been published.</td>
</tr>
</tbody>
</table>

### Council of Roots
- CVE
- CVE Board
- CVE Identifier (CVE ID)
- CVE List
- CVE Numbering Authority (CNA)
- CVE Numbering Authority of Last Resort (CNA-LR)
- CVE Program
- CVE Record
- CVE Working Group
- End of Life (EOL)

### Fix
- Independently Fixable
- Product
- Publicly Disclosed

### Reserved but Public (RBP)
- Root
- Scope
- Secretariat
- Supplier
- Tags
- Top-Level Root (TL-Root)
- Vulnerability

Provide feedback for this page
WHO I AM AND WHAT I DO

I issue CVE IDs to vulnerabilities.

I review other CNAs’ CVE IDs for inclusion in the GitHub Advisory Database.

I have to deal with excess CVE IDs at the end of the year – my org’s as well as others’.
GitHub Advisory Database

Security vulnerability database inclusive of CVEs and GitHub originated security advisories from the world of open source software.

GitHub reviewed advisories

<table>
<thead>
<tr>
<th>Package</th>
<th>Advisories</th>
</tr>
</thead>
<tbody>
<tr>
<td>All reviewed</td>
<td>17,086</td>
</tr>
<tr>
<td>Composer</td>
<td>2,855</td>
</tr>
<tr>
<td>Erlang</td>
<td>26</td>
</tr>
<tr>
<td>GitHub Actions</td>
<td>16</td>
</tr>
<tr>
<td>Go</td>
<td>1,532</td>
</tr>
<tr>
<td>Maven</td>
<td>4,824</td>
</tr>
<tr>
<td>npm</td>
<td>3,352</td>
</tr>
<tr>
<td>NuGet</td>
<td>578</td>
</tr>
<tr>
<td>pip</td>
<td>2,511</td>
</tr>
<tr>
<td>Pub</td>
<td>8</td>
</tr>
<tr>
<td>RubyGems</td>
<td>814</td>
</tr>
<tr>
<td>Rust</td>
<td>747</td>
</tr>
</tbody>
</table>

Search by CVE/GHSA ID, package, severity, ecosystem, credit...

17,086 advisories

- **CLI for Vela Insecure Variable Substitution** (High)
  GHSA-4hj-3gv3-c3gr was published for github.com/go-vela/cli (Go) yesterday

- **Golang SDK for Vela Insecure Variable Substitution** (High)
  GHSA-v8mx-hp2q-gw85 was published for github.com/go-vela/sdk-go (Go) yesterday

- **Server/API for Vela Insecure Variable Substitution** (High)
  GHSA-69p4-j5v5-x234 was published for github.com/go-vela/server (Go) yesterday

- **Types for Vela Insecure Variable Substitution** (High)
  GHSA-7v38-w32m-wx4m was published for github.com/go-vela/types (Go) yesterday

- **tls-listener affected by the slow loris vulnerability with default configuration** (High)
  CVE-2024-28854 was published for tis-listener (Rust) yesterday

- **TurboBoost Commands vulnerable to arbitrary method invocation** (High)
  CVE-2024-28181 was published for @turbo/boost/commands (RubyGems) yesterday
MY PRE-GITHUB WORK

Shelby Cunningham
Get Hip Recordings
Jan 2020 - Mar 2021
gethip.com/store
When I originally joined GitHub, my team was a new CNA responsible for all the tasks related to our advisory database and CNA obligations.

Shelby Cunningham
GitHub Advisory Database Curator
github.com/shelbyc
When I originally joined GitHub, my team was a relatively new CNA responsible for all the tasks related to our advisory database and CNA obligations.

On top of that, we dealt with a huge piece of news for a lot of advisory databases: the fallout of log4j around Dec 2021 - Jan 2022.
MY PRE-GITHUB WORK

github.com/shelbyc
THAT RECORD STORE JOB HELPED MY CYBERSECURITY CAREER

Shelby Cunningham
GitHub Advisory Database Curator
github.com/shelbyc
That record store job helped my cybersecurity career

Shelby Cunningham
GitHub Advisory Database Curator
github.com/shelbyc

Some lower-priority tasks (such as rejecting unused CVEs) fell through the cracks.
Some lower-priority tasks (such as rejecting unused CVEs) fell through the cracks.

On top of that, everything related to handling CVEs was a manual process until 2022.

A human had to double check everything.
THAT RECORD STORE JOB HELPED MY CYBERSECURITY CAREER

Shelby Cunningham
GitHub Advisory Database Curator
github.com/shelbyc
At the end of 2022, I took on rejecting GitHub’s unused CVEs at the end of the year for the first time.
At the end of 2022, I took on rejecting GitHub’s unused CVEs at the end of the year for the first time.

This ended up being a bigger project than I had anticipated.
At the end of 2022, I took on rejecting GitHub’s unused CVEs at the end of the year for the first time.

This ended up being a bigger project than I had anticipated.

I discovered CVEs that had been made public but not published when checking CVE spreadsheet manually.
Welcome to the new CVE Beta website! CVE Records have a new and enhanced format. View records in the new format using the CVE ID lookup above or download them on the Downloads page. The search will be temporarily hosted on the legacy cve.mitre.org website until the transition is complete.

## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reserved but Public (RBP)</strong></td>
<td>A CVE ID in the “Reserved” state that is referenced in one or more public sources but for which a CVE Record has not been published.</td>
</tr>
</tbody>
</table>

### Council of Roots
- CVE
- CVE Board
- CVE Identifier (CVE ID)
- CVE List
- CVE Numbering Authority (CNA)
- CVE Numbering Authority of Last Resort (CNA-LR)
- CVE Program
- CVE Record
- CVE Working Group
- End of Life (EOL)

### Fix
- Independently Fixable
- Product
- Publicly Disclosed

### Reserved but Public (RBP)
- Root
- Scope
- Secretariat
- Supplier
- Tags
- Top-Level Root (TL-Root)
- Vulnerability

Provide feedback for this page
Why worry about excess Reserved CVEs?
Data timeliness and relevance
Data transparency
Minimize deluges of new records at the end of a quarter or year
Minimize confusion from other CNAs unknowingly assigning duplicate CVEs
Letting CVE information sit can lead to link rot or other information loss.
New rules say so
Section 4.5 of new (but not yet final) CVE CNA rules

4.5.1.4 CNAs MUST publish a CVE Record to the CVE List within 72 hours of Publicly Disclosing a CVE ID assigned by the CNA. If the CNA does not publish within 72 hours, then the CNA’s Root MAY direct the appropriate CNA-LR to publish a CVE Record for the assigned CVE ID.
Section 4.5 of new (but not yet final) CVE CNA rules

This means if you don’t publish the CVE record within 72 hours, the CVE record gets taken away from your CNA!
Section 4.5 of new (but not yet final) CVE CNA rules

4.5.1.6 CNAs SHOULD publish CVE Records within 72 hours of becoming aware that a CVE ID assigned by the CNA has been Publicly Disclosed by a party other than the CNA.
Techniques to Minimize Accumulation of Excess Reserved CVEs
Request CVEs on an as-needed basis.
“But what if our API connection breaks down and we need a buffer of CVEs?”
Request smaller, more frequent batches of CVEs.

How many CVEs does your org issue in...
Request smaller, more frequent batches of CVEs.

How many CVEs does your org issue in... ...a month?
Request smaller, more frequent batches of CVEs.

How many CVEs does your org issue in... 
... a month? ... a week?
Request smaller, more frequent batches of CVEs.

How many CVEs does your org issue in... 
... a month? 
... a week? 
... a day?
Request smaller, more frequent batches of CVEs.

How many CVEs does your org issue in...
... a month?
... a week?
... a day?
... one project?
Request smaller, more frequent batches of CVEs.

Batches don’t have to be the same size for each request.
The Downside:
The Downside:

Vulnerabilities that become public without a CVE being assigned immediately risk another CNA assigning a duplicate CVE.
Populate CVE records as soon as reasonably possible.
GHSL-2021-1045: Cross-Site Scripting (XSS) in jQuery MiniColors Plugin - CVE-2021-32850

GitHub Security Lab

Coordinated Disclosure Timeline

- 2021-11-24: Maintainer contacted
- 2021-11-24: Maintainer fixed the issue
QUICK INFO

CVE Dictionary Entry:
CVE-2021-32850

NVD Published Date:
02/20/2023

NVD Last Modified:
11/06/2023

Source:
GitHub, Inc.
CVE-2021-4243 Detail

REJECTED

CVE has been marked "REJECT" in the CVE List. These CVEs are stored in the NVD, but do not show up in search results.

Current Description

Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-32850. Reason: This candidate is a duplicate of CVE-2021-32850. Notes: All CVE users should reference CVE-2021-32850 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
Publishing ASAP has the added benefit of keeping information in newly-published CVEs timely and actionable.
CVE consumers’ holiday season when CNAs wait until the end of the quarter and/or year to publish
CVE consumers’ holiday season when CNAs don’t publish huge batches at the end of the quarter/year
Have and enforce a disclosure policy, preferably with a timeline or milestone to achieve that triggers publication.
**Timeline examples**

- 90 days after discovery
- 30 days after a fix is developed to give users time to patch

**Milestone examples**

- When a patch is available
- When the vulnerability becomes public knowledge, e.g. in a researcher blog
Have playbooks and checklists for the necessary processes, especially if disclosure is not a routine process!
Check if any CVEs marked “Reserved But Public” have been disclosed publicly.
GHSL-2021-1045: Cross-Site Scripting (XSS) in jQuery MiniColors Plugin - CVE-2021-32850

GitHub Security Lab

Coordinated Disclosure Timeline

- 2021-11-24: Maintainer contacted
- 2021-11-24: Maintainer fixed the issue
QUICK INFO

CVE Dictionary Entry:
CVE-2021-32850

NVD Published Date:
02/20/2023

NVD Last Modified:
11/06/2023

Source:
GitHub, Inc.
Lessons learned cleaning up my CNA’s CVEs
Lessons learned cleaning up my CNA’s CVEs

The rules are there for a reason.
Lessons learned cleaning up my CNA’s CVEs

The rules are there for a reason.

Staying on top of CVEs and preventing RBP backlogs is less work than clearing backlogs.
Lessons learned cleaning up my CNA’s CVEs

The rules are there for a reason.

Staying on top of CVEs and preventing RBP backlogs is less work than clearing backlogs.

But going from falling behind to on top of your CNA’s CVEs is worthwhile!
Lessons learned cleaning up my CNA’s CVEs

Different CNAs should use different combinations of techniques so that their orgs can minimize RBP CVEs in a way that works for them.
Lessons learned cleaning up my CNA’s CVEs

Different CNAs should use different combinations of techniques so that their orgs can minimize RBP CVEs in a way that works for them.

Within the same CNA, the techniques that work best may change over time.
Lessons learned cleaning up my CNA’s CVEs

Manual recordkeeping might be less money to develop but costs human effort. Is it worth your org’s money to develop automated tooling?
NextChat: An AI Chatbot That Lets You Talk to Anyone You Want To

by Naveen Sunkavally [Mar 11, 2024] Attack Blogs, Disclosures

With the advent of generative AI, AI chatbots are everywhere. While users can chat with large-language models (LLMs) using a SaaS provider like OpenAI, there are lots of standalone chatbot applications available for users to deploy and use too. These standalone applications generally offer a richer user interface than OpenAI, additional features such as the ability to plug in and test different models, and the ability to potentially bypass IP block restrictions.

From our research, the most widely deployed standalone Gen AI chatbot is NextChat, a.k.a ChatGPT-Next-Web. This is a GitHub project with 63K+ stars and 52K+ forks. The Shodan query title:NextChat, "ChatGPT Next Web" pulls up 7500+ exposed instances, mostly in China and the US.

This application is vulnerable to a critical full-read server-side request forgery (SSRF) vulnerability, CVE-2023-49785, that we disclosed to the vendor in November 2023. As of this writing, there is no patch for the vulnerability, and since 90+ days has passed since our original disclosure, we are now releasing full details here.
**CVE-2023-49785 Detail**

**AWAITING ANALYSIS**

This vulnerability is currently awaiting analysis.

**Description**

NextChat, also known as ChatGPT-Next-Web, is a cross-platform chat user interface for use with ChatGPT. Versions 2.11.2 and prior are vulnerable to server-side request forgery and cross-site scripting. This vulnerability enables read access to internal HTTP endpoints but also write access using HTTP POST, PUT, and other methods. Attackers can also use this vulnerability to mask their source IP by forwarding malicious traffic intended for other Internet targets through these open proxies. As of time of publication, no patch is available, but other mitigation strategies are available. Users may avoid exposing the application to the public internet or, if exposing the application to the internet, ensure it is an isolated network with no access to any other internal resources.
Lessons learned cleaning up my CNA’s CVEs

Manual recordkeeping might be less money to develop but costs human effort. Is it worth your org’s money to develop automated tooling?

Clearing backlogs of CVE records for a CNA pays way better than clearing backlogs of sales records for a music distro.
SPECIAL THANKS TO MY TEAMMATES

Jonathan Evans (@jonathanlevans)

Madison Oliver (@taladrane)

Jon Moroney (@darakian)

Chamari McLean (@callmemari)

The GitHub Security Lab
(https://securitylab.github.com/)
Do we have other lights except for these real brights...

...these astro brights...

Q&A

security-advisories@github.com

metalhead.club/@scunning

Credit: Heather Mull and Dan Barnhill