

VULNRICHMENT YEAR ONE

Lindsey Cerkovnik
Branch Chief
CISA VRC

Art Manion
Deputy Director
ANALYGENCE Labs

With thanks (and
possibly apologies) to
Tod Beardsley



CISA Vulnerability Management

- **VM Mission** | Reduce the prevalence and impact of vulnerabilities and exploitable conditions across enterprises and technologies, including through assessments and coordinated disclosure of vulnerabilities reported by trusted partners.
- **Stakeholders** | Federal, Civilian, Executive Branch (FCEB) Agencies; State, Local, Tribal, and Territorial (SLTT) Governments; and Critical Infrastructure (CI).



CVD, KEV, CSAF, SSSVC

```
{
  "title": "CISA Catalog of Known Exploited Vulnerabilities",
  "catalogVersion": "2025.04.07",
  "dateReleased": "2025-04-07T18:01:08.3813Z",
  "count": 1315,
  "vulnerabilities": [
    {
      "cveID": "CVE-2025-31161",
      "vendorProject": "CrushFTP",
      "product": "CrushFTP",
      "vulnerabilityName": "CrushFTP Authentication Bypass Vulnerability",
      "dateAdded": "2025-04-07",
      "shortDescription": "CrushFTP contains an authentication bypass vulnerability in the HTTP authentication that allows a remote unauthenticated attacker to authenticate to any known or guessable user account (e.g. potentially leading to a full compromise.",
      "requiredAction": "Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidelines, or discontinue use of the product if mitigations are unavailable.",
      "dueDate": "2025-04-28",
      "knownRansomwareCampaignUse": "Unknown",
      "notes": "https://www.crushftp.com/crush1wiki/Wiki.jsp?page=Update ; https://nvd.nist.gov/vuln/detail/CVE-2025-31161",
      "cwes": [
        "CWE-305"
      ]
    },
    {
      "cveID": "CVE-2025-31162",
      "vendorProject": "Conn",
      "product": "Conn",
      "vulnerabilityName": "Conn",
      "dateAdded": "2025-04-07",
      "shortDescription": "Conn contains a buffer overflow vulnerability that allows a remote unauthenticated attacker to cause a denial of service.",
      "requiredAction": "Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidelines, or discontinue use of the product if mitigations are unavailable.",
      "dueDate": "2025-04-28",
      "knownRansomwareCampaignUse": "Unknown",
      "notes": "CISA Memorandum of Understanding for the Secure-ZTA-Gateways-CVE-2025-31162",
      "cwes": [
        "CWE-121"
      ]
    }
  ]
}
```

Coordinated Vulnerability Disclosure Process

CISA's CVD program coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with the affected vendor(s). This includes new vulnerabilities in industrial control systems (ICS), Internet of Things (IoT), and medical devices, as well as traditional information technology (IT) vulnerabilities. The goal of CISA's CVD program is to ensure that CISA, the affected vendor(s) and/or service provider(s), and the vulnerability reporter all disclose simultaneously, to ensure that users and administrators receive clear and actionable information in a timely manner.

Read our blog that discusses how cybersecurity researchers have a valuable role in this effort and encourages organizations to engage with them. [Engaging with Security Researchers: Embracing a "See Something, Say Something" Culture](#), published October 23, 2024.

CISA CSAF Repository

The purpose of this repository is to provide machine-readable security advisories using [Common Security Advisory Framework \(CSAF\) Version 2.0 standard](#) for CISA's Information Technology (IT) and Operational Technology (OT) advisories. By providing machine-readable advisories in v2.0, vendors and providers of software and hardware can join [CISA and many other leading organizations](#) in taking [proactive steps to enable automation and help to reduce the time for enterprises to understand organizational impact and drive timely remediation.](#)



CISA Stakeholder-Specific Vulnerability Categorization Guide

Publication: November 2022
Cybersecurity and Infrastructure Security Agency



Design goals

Goal

Implementation

Provide useful data for vulnerability management

SSVC, KEV, CVSS, CWE, ~~CPE~~

Leverage existing capabilities

CISA vulnerability triage and analysis, CVE ecosystem, first production ADP

Transparency

Public repository, documentation, resolve issues and change requests

Accuracy

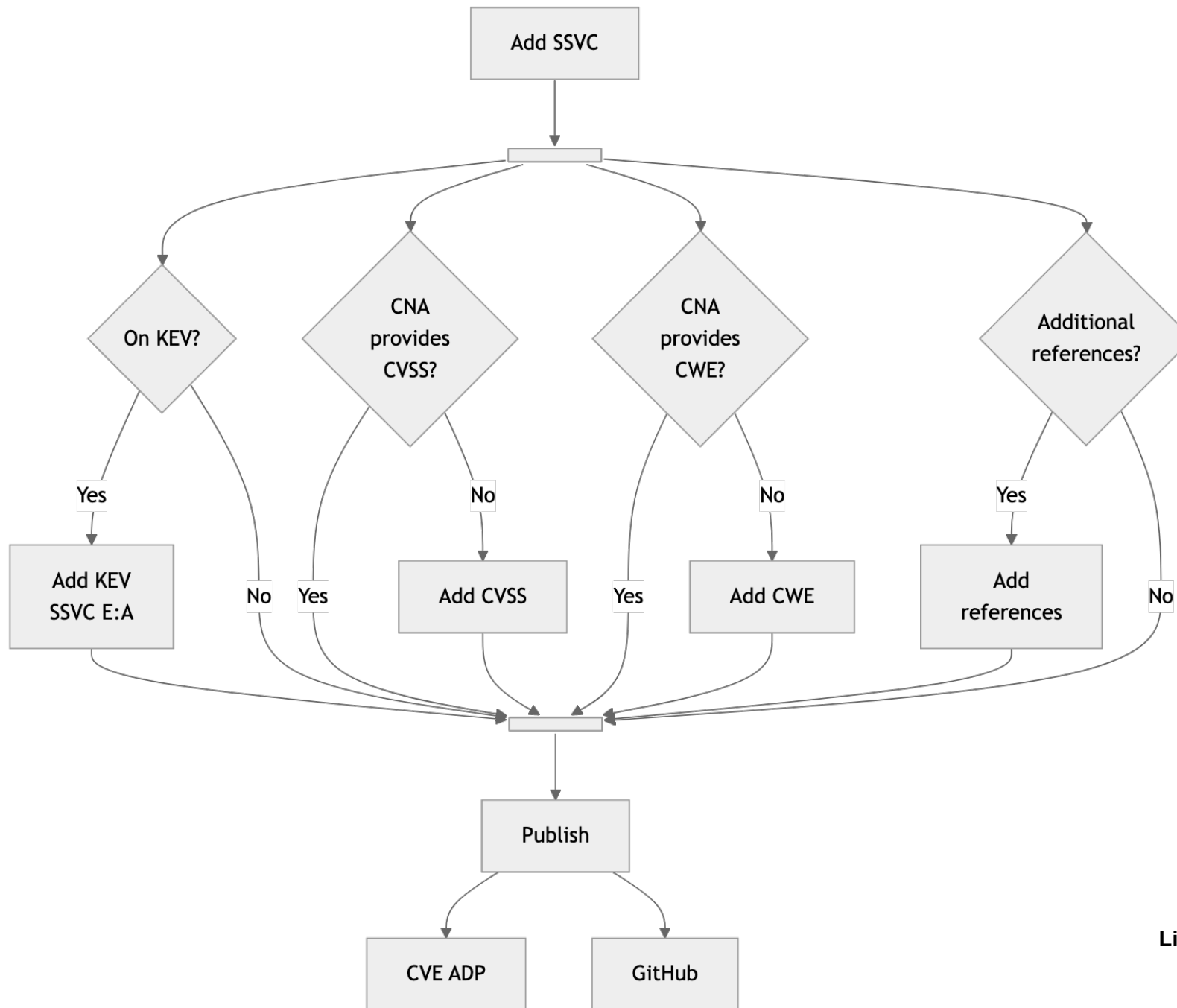
Do not override CNA, easy to request changes



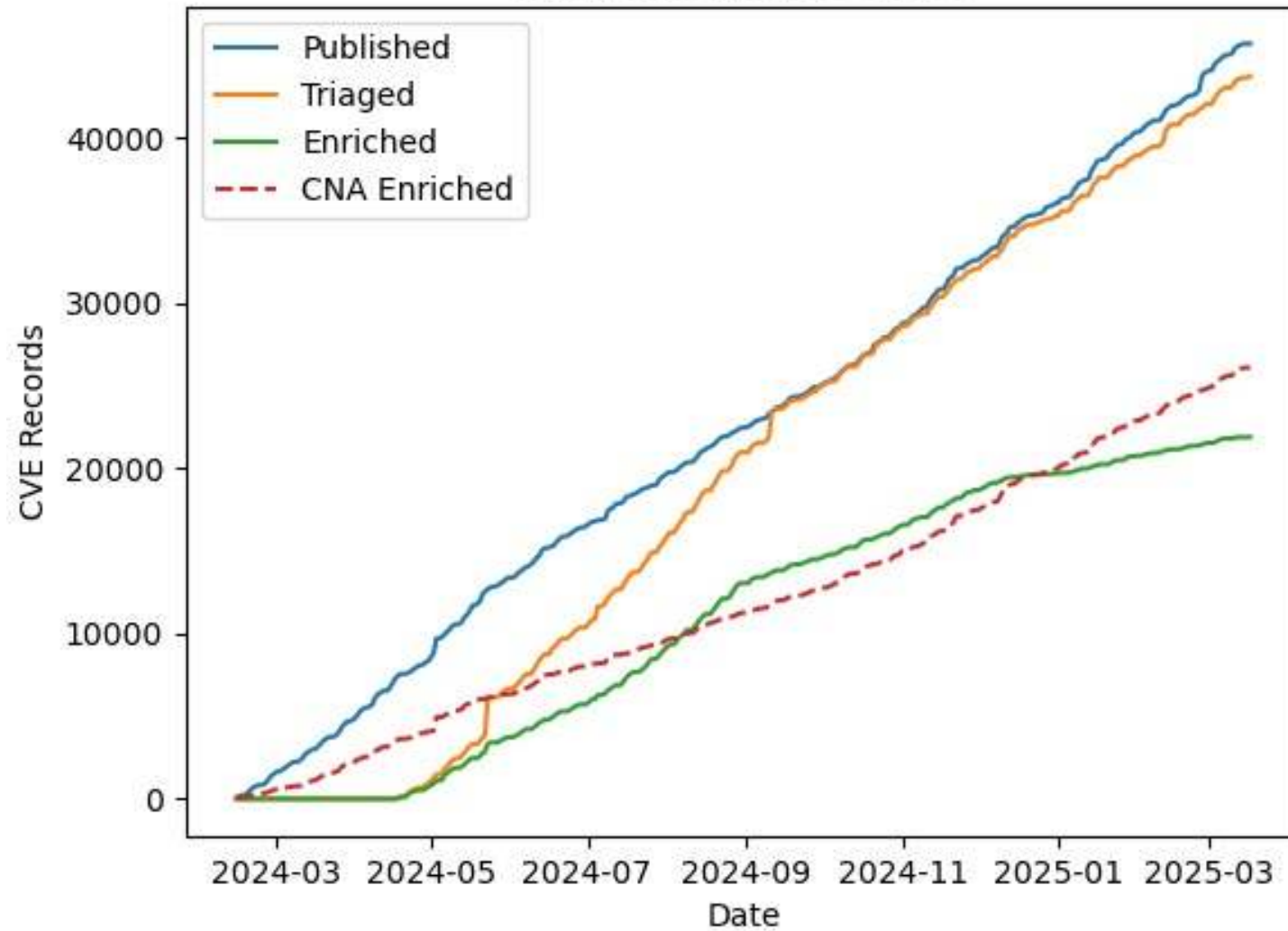
Information sources

Information	Source
SSVC	CISA
KEV	CISA
CVSS	CNA or CISA
CWE	CNA or CISA
Additional references	CNA and CISA
CPE	CNA and NVD





Vulnrichment by the numbers



Tooling for transparency

📖 README 🔒 CC0-1.0 license 🔒 Security ✎ ☰

CISA Vulnrichment

The CISA Vulnrichment project is the public repository of CISA's enrichment of public CVE records through CISA's ADP (Authorized Data Publisher) container. In this phase of the project, CISA is assessing new and recent CVEs and adding key [SSVC](#) decision points. Once scored, some higher-risk CVEs will also receive enrichment of [CWE](#) and/or [CVSS](#) data points, where possible.

Issues and pull requests

We want to hear from you, the IT cybersecurity professional community, about Vulnrichment and ADP! If you see something, please feel free to say something in the [Issues](#), or even better, open a [pull request](#) with your suggested fix. Note that if you have an issue with the data from the CNA container, you are encouraged to take that issue up with the [responsible CNA](#) directly.



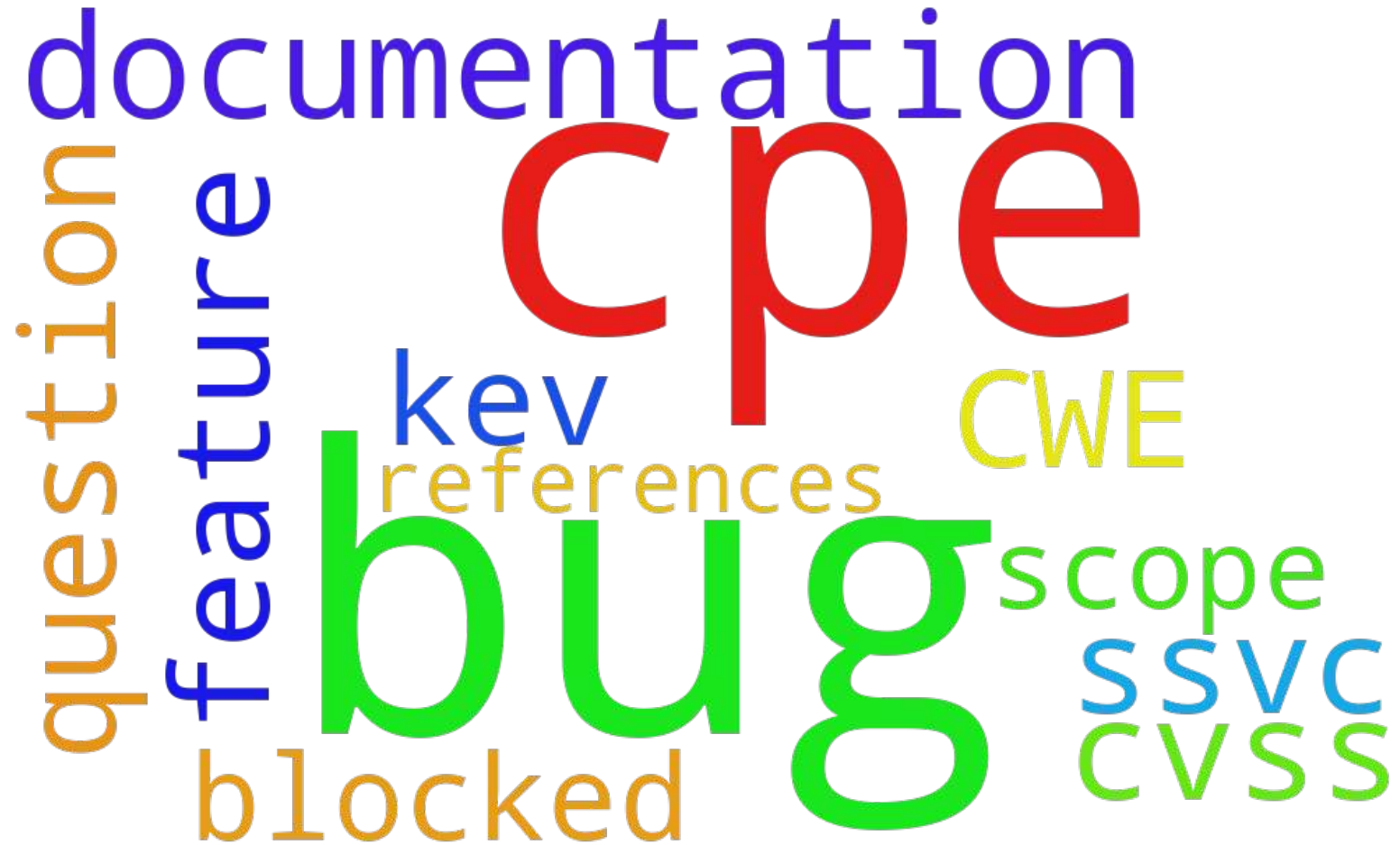
Transparency by the numbers

Information	Source
Issues	2 open, 97 closed
Pull requests	0 open, 67 closed
Forks	62
Average comments	2.1
Average days open	6.5
CVSS arguments	2 fought, 0 won



Labels

blocked	4
bug	170
cpe	108
cvss	40
CWE	28
documentation	64
feature	24
key	12
out of scope	2
question	18
references	2
ssvc	28



Lessons Learned: CVSS

Update CVE-2025-22376 following independent review #154

Merged

jwoytek-cisa m

Conversation 12

psyker156 commen

I did an independent
for what the vulnera
explains the rational
blog post as a refere



amanion-cisa commented on Jan 21 · edited

Collaborator

We're going to accept your CVSS score, thanks for the analysis and for filing a PR.

While I question the value of debating CVSS scores, especially for library vulnerabilities, I'll carry on a bit further. CVSS (3.1 and 4.0) guidance talks about the "reasonable worst-case," particularly in regard to the [abstraction level of libraries](#), and this comes from a history of assuming worst-case impact. I agree that data integrity is not directly impacted, but might argue that cryptographic integrity is, therefore I:L. Assuming an attacker can intercept a request (HTTP GET, or no TLS, or intercepting TLS), accurately enough guess timestamps, and work within time/state windows, it seems that being able to predict nonces would contribute to the attacker's ability to pull off a replay attack (predict a recently-enough used nonce). Certainly depends on application behavior, and I wouldn't extent the CVSS impact to user account or session compromise.

Labels

bug

cvss

Update CVE-2025-22376 following independent review

ae3c67b



Lindsey Cerkovnik
Art Manion
April 8, 2025


Lessons Learned: Community

CVE-2024-11053.json: adjusted CVSS scoring: MEDIUM 5.3 #151

Edit <> Code ▾

 Closed bagder wants to merge 1 commit into `cisagov:develop` from `bagder:CVE-2024-11053` 

Conversation 3 Commits

 bagder commented on Dec 15, 2024

The security problem this descr
accidentally stumble upon this.


- "vectorString": "CVSS:3.1/A"


 bagder commented on Dec 15, 2024


fixed already



  bagder closed this on Dec 15, 2024

+8 -8 







Lindsey Cerkovnik
Art Manion
April 8, 2025

Lessons Learned: CPE

Vulnrichment provided

- A committed experim

It's possible to generate

- But is it correct? Who
- As designed, only the

- CVE Record Format
- Distracted from core

Who uses CPE? Who u

- Feedback that Vulnric

Some explanation, which may or may not address the specific instances you noticed (which we will review!).

CPE strings must match NVD, where possible.

Yes, and this is how the process is designed to work. And...

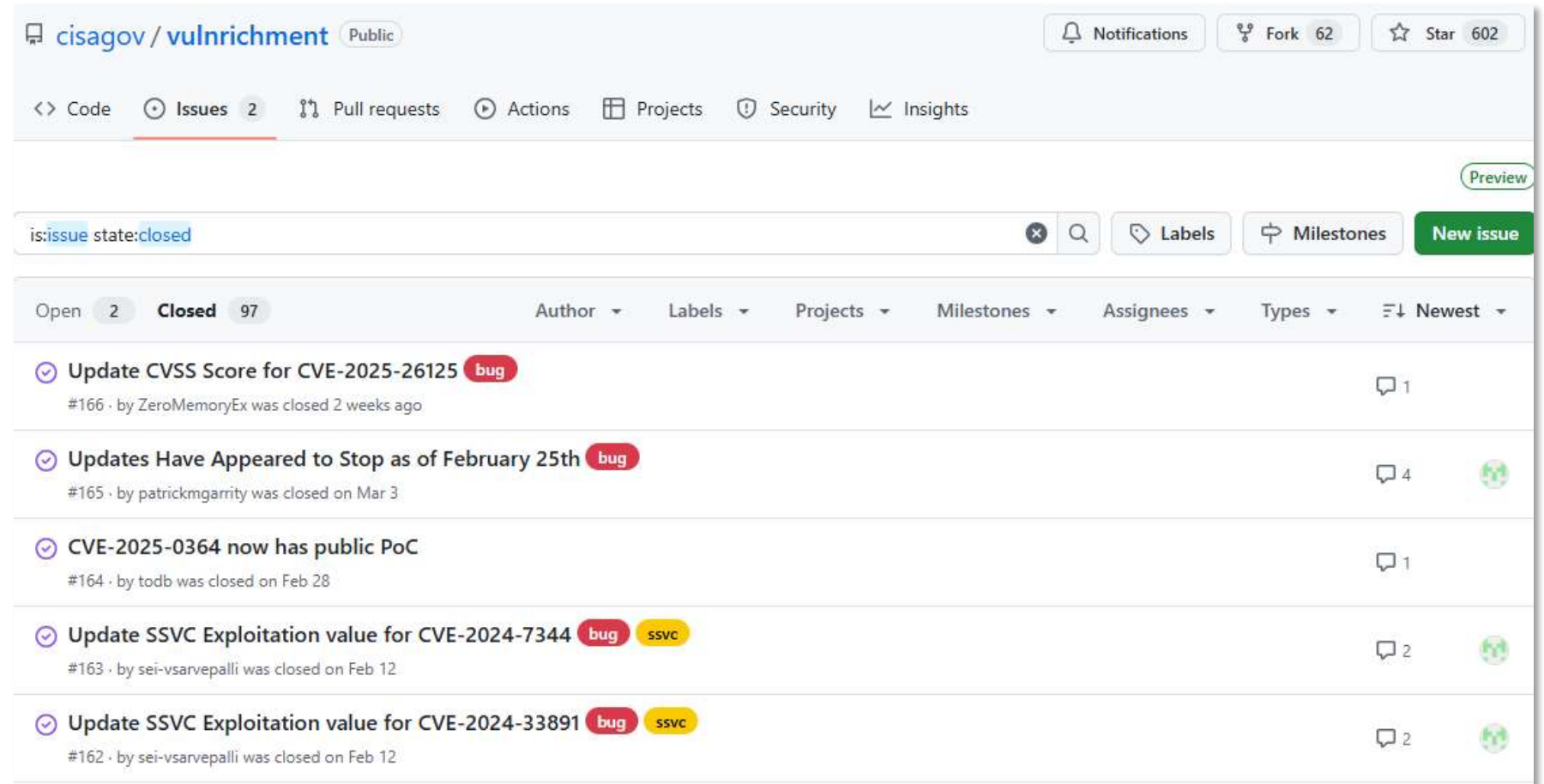
1. There is the official [NVD CPE Dictionary](#). First choice. However, even that has matching issues, for example, [some xpdf entries](#) use `xpdfreader` as the vendor.
2. Next, there are a number (84K+) of CPE entries in NVD data that are not in the Dictionary (1.2M+). Second choice (use something that exists).
3. Last choice is to create new CPE. In this sense, we're following the [CPE specification](#), but publishing CPE-compliant data does not get it added to the Dictionary.

Let's be clear, CPE is an attempt to address the wicked problem that is consistently naming all the software. Neither the CPE specification nor existing CPE data can do this, but it's a start, and an existing data set (or sets). There will be errors, and part of this process is to evaluate how CPE or other software identification systems work in practice.



Future

- Continued community engagement and transparency
- CISA VM mission as a public service
- “Test in production” experiments (CPE, SSVC, what else?)



The screenshot shows the GitHub interface for the repository 'cisagov/vulnrichment'. The repository is public and has 62 forks and 602 stars. The 'Issues' tab is selected, showing a search bar with the query 'is:issue state:closed'. Below the search bar, there are filters for 'Open' (2) and 'Closed' (97) issues. The list of issues includes:

- Update CVSS Score for CVE-2025-26125 (bug) - #166 - by ZeroMemoryEx was closed 2 weeks ago
- Updates Have Appeared to Stop as of February 25th (bug) - #165 - by patrickmgarrity was closed on Mar 3
- CVE-2025-0364 now has public PoC - #164 - by todob was closed on Feb 28
- Update SSVC Exploitation value for CVE-2024-7344 (bug, ssvc) - #163 - by sei-vsarvepalli was closed on Feb 12
- Update SSVC Exploitation value for CVE-2024-33891 (bug, ssvc) - #162 - by sei-vsarvepalli was closed on Feb 12





Thanks!

<https://www.cisa.gov>

<https://github.com/cisagov/vulnrichment>