# Уязвимости как потоки данных

Юлия Волкова
Дата-человек в CodeScoring

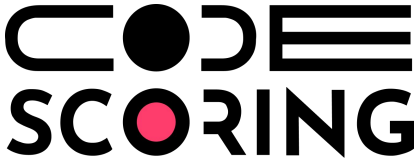
# О спикере

Head of Data @ CODE SCORING

https://github.com/xnuinside

Юля Волкова

# Масштаб “бедствия”




Работаем с:

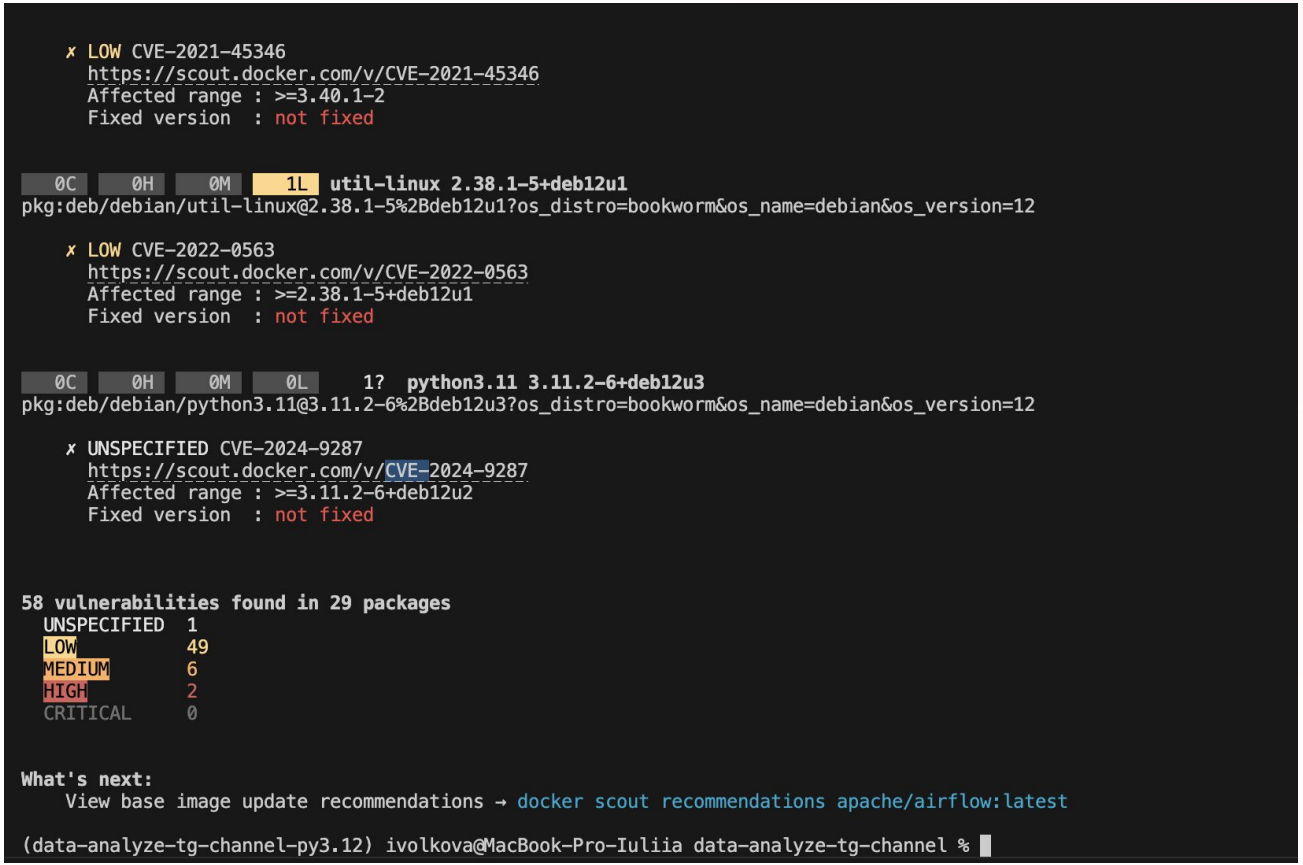
- Java
- Python
- Golang
- Rust
- PHP
- JavaScript
- .NET
- Ruby
- и др

- Alpine
- Debian
- Ubuntu
- Red Hat
- и др

# О чем доклад

Сканеры уязвимостей
и их **источники данных***

**с большим уклоном в open source*


✗ LOW CVE-2021-45346
https://scout.docker.com/v/CVE-2021-45346
Affected range : >=3.40.1-2
Fixed version : not fixed
0C 0H 0M 1L util-linux 2.38.1-5+deb12u1
pkg:deb/debian/util-linux@2.38.1-5%2Bdeb12u1?os_distro=bookworm&os_name=debian&os_version=12
✗ LOW CVE-2022-0563
https://scout.docker.com/v/CVE-2022-0563
Affected range : >=2.38.1-5+deb12u1
Fixed version : not fixed
0C 0H 0M 0L 1? python3.11 3.11.2-6+deb12u3
pkg:deb/debian/python3.11@3.11.2-6%2Bdeb12u3?os_distro=bookworm&os_name=debian&os_version=12
✗ UNSPECIFIED CVE-2024-9287
https://scout.docker.com/v/CVE-2024-9287
Affected range : >=3.11.2-6+deb12u2
Fixed version : not fixed
58 vulnerabilities found in 29 packages
UNSPECIFIED 1
LOW 49
MEDIUM 6
HIGH 2
CRITICAL 0
What's next:
View base image update recommendations → docker scout recommendations apache/airflow:latest
(data-analyze-tg-channel-py3.12) ivolkova@MacBook-Pro-Iuliia data-analyze-tg-channel %

# Vulnerability Scanners
(Open Source only)

[command line tools]

1. Trivy - https://trivy.dev/
2. Grype - https://github.com/anchore/grype
3. Docker scout - https://docs.docker.com/scout/
4. OWASP Dep-scan - https://owasp.org/www-project-dep-scan/
5. DependencyCheck - https://github.com/jeremylong/DependencyCheck

[servers]

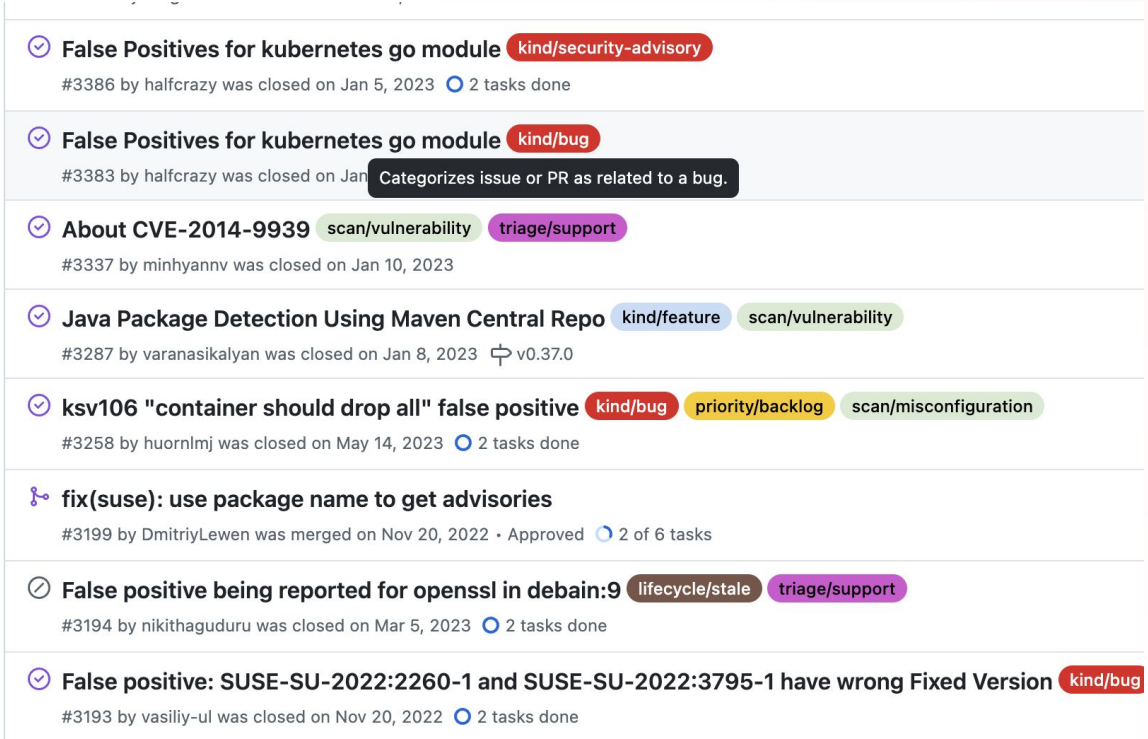
1. Clair - https://github.com/quay/clair
2. Anchore Engine* - https://github.com/anchore/anchore-engine
3. Dagda - https://github.com/eliasgranderubio/dagda

*deprecated

# Цель

Понять откуда растут ноги у фолзов (и принять)

# Фолзят все




https://github.com/aquasecurity/trivy/issues?page=4&q=false+positive

# Фолзят все

## Suppressing False Positives

Due to how dependency-check identifies libraries false positives may occur (i.e. a CPE was identified that is incorrect). Suppressing these
next to each CPE identified (and on CVE entries) there is a suppress button. Clicking the suppression button will create a dialogue box wh
place into a suppression XML file. If this is the first time you are creating the suppression file you should click the “Complete XML Doc” b
elements.

A sample suppression file would look like:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<suppressions xmlns="https://jeremylong.github.io/DependencyCheck/dependency-suppression.1.3.xsd">
   <suppress>
      <notes><![CDATA[
      file name: some.jar
      ]]></notes>
      <sha1>66734244CE86857018B023A8C56AE0635C56B6A1</sha1>
      <cpe>cpe:/a:apache:struts:2.0.0</cpe>
   </suppress>
</suppressions>
```

The above XML file will suppress the cpe:/a:apache:struts:2.0.0 from any file with the a matching SHA1 hash.

The following shows some other ways to suppress individual findings. Note the ways to select files using either the sha1 hash or the fileP
things that can be suppressed - individual CPEs, individual CVEs, or all CVE entries below a specified CVSS score. The most common w
(regexes) - these entries can be generated using the HTML version of the report. The other common scenario would be to ignore all CVEs

```xml
<?xml version="1.0" encoding="UTF-8"?>
<suppressions xmlns="https://jeremylong.github.io/DependencyCheck/dependency-suppression.1.3.xsd">
    <suppress>
        <notes><![CDATA[
```

https://jeremylong.github.io/DependencyCheck/general/suppression.html

# Фолзят все

- False positive: GHSA-qhch-g8qr-p497 (CVE-2014-3641) cinder 17.4.1.x, recommend fixed with 2014.x older versioning convention. bug needs-discussion
  #2240 opened 5 days ago by sekveaja
- Conflicting config defaults documentation
  #2239 opened 5 days ago by benjaminwilcox
- False positive: GHSA-cx63-2mw6-8hw5 (CVE-2024-6345) python311-setuptools in SLES 15.5 Ecosystem cause by Syft noise with extra reference bug false-positive
  #2210 opened 2 weeks ago by sekveaja
- False positives for recent CUPS vulnerability CVE-2024-47175 bug needs-discussion
  #2156 opened on Oct 3 by dbrugman
- False positive: CVE-2023-47100 (duplicate of CVE-2023-47038) in perl-5.36.2 bug changelog-ignore false-positive
  #2137 by nielsaka was closed on Sep 23
- False Positive: GHSA-j225-cvw7-qrx7 (CVE-2023-52323) python3-pycryptodome bug false-positive
  #2068 opened on Aug 20 by sekveaja
- False Positive: GHSA-jfmj-5v4g-7637 (CVE-2024-5569) python3-zipp due to Syft noise and mismatch of package name bug false-positive
  #2061 opened on Aug 15 by sekveaja

https://github.com/anchore/grype/issues?q=false+positive

# “Компоненты” сканера

Какая-то логика получения списка ПО - версия

*Что мы проверяем? В чем ищем уязвимости?*

# **SBOM** (Software Bill of Materials)


```
    {
      "type": "library",
      "bom-ref": "pkg:maven/org.bouncycastle/bcprov-jdk15on@1.62?type=jar",
      "group": "org.bouncycastle",
      "name": "bcprov-jdk15on",
      "version": "1.62",
      "description": "The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms.
This jar contains JCE provider and lightweight API for the Bouncy Castle Cryptography APIs for JDK 1.5 to JDK 1.8.",
      "hashes": [
        {
          "alg": "MD5",
          "content": "01b1a8cff910fdb9328cef5c437ff2f9"
        },
{
          "alg": "SHA-256",
          "content": "2fa0ab71b154da29ac134097bc6bbacd90987dd4c4005516159e6494d1d52ea2"
        },...
      ],
      "licenses": [{"license": {
        "name": "Bouncy Castle Licence",
        "url": "http://www.bouncycastle.org/licence.html"
      }}],
      "purl": "pkg:maven/org.bouncycastle/bcprov-jdk15on@1.62?type=jar",
      "externalReferences": [
        {
          "type": "issue-tracker",
          "url": "https://github.com/bcgit/bc-java/issues"
        },
        {
          "type": "vcs",
          "url": "https://github.com/bcgit/bc-java"
        }
      ]
    },
    {
      "type": "library",
      "bom-ref": "pkg:maven/org.bouncycastle/bcpkix-jdk15on@1.62?type=jar",
      "group": "org.bouncycastle",
      "name": "bcpkix-jdk15on",
      "version": "1.62",
```


пример взят с:
https://raw.githubusercontent.com/CycloneDX/bom-examples/refs/heads/master/SBOM/keycloak-10.0.2/bom.json

# **SBOM** (Software Bill of Materials)

```
"components": [
    {
      "type": "library",
      "purl":
"pkg:maven/org.bouncycastle/bcprov-jdk15on@1.62?type=jar",
      "group": "org.bouncycastle",
      "name": "bcprov-jdk15on",
      "version": "1.62",
      "description": "The Bouncy Castle Crypto package is a Java
implementation of cryptographic algorithms.
This jar contains JCE provider and lightweight API for the
Bouncy Castle Cryptography APIs for JDK 1.5 to JDK 1.8.",
```

пример взят с:
https://raw.githubusercontent.com/CycloneDX/bom-examples/refs/heads/master/SBOM/keycloak-10.0.2/bom.json

# ЧТО ТАКОЕ PURL(Package URL)

CODE SCORING

```
pkg:maven/org.bouncycastle/bcprov-jdk15on@1.62?type=jar
```

Спецификация:
https://github.com/package-url/purl-spec/blob/master/PURL-SPECIFICATION.rst

# PURL(Package URL):Debian

```
pkg:deb/debian/0install@2.12.3-2?arch=amd64&distro=debian-10
&upstream=zeroinstall-injector
```

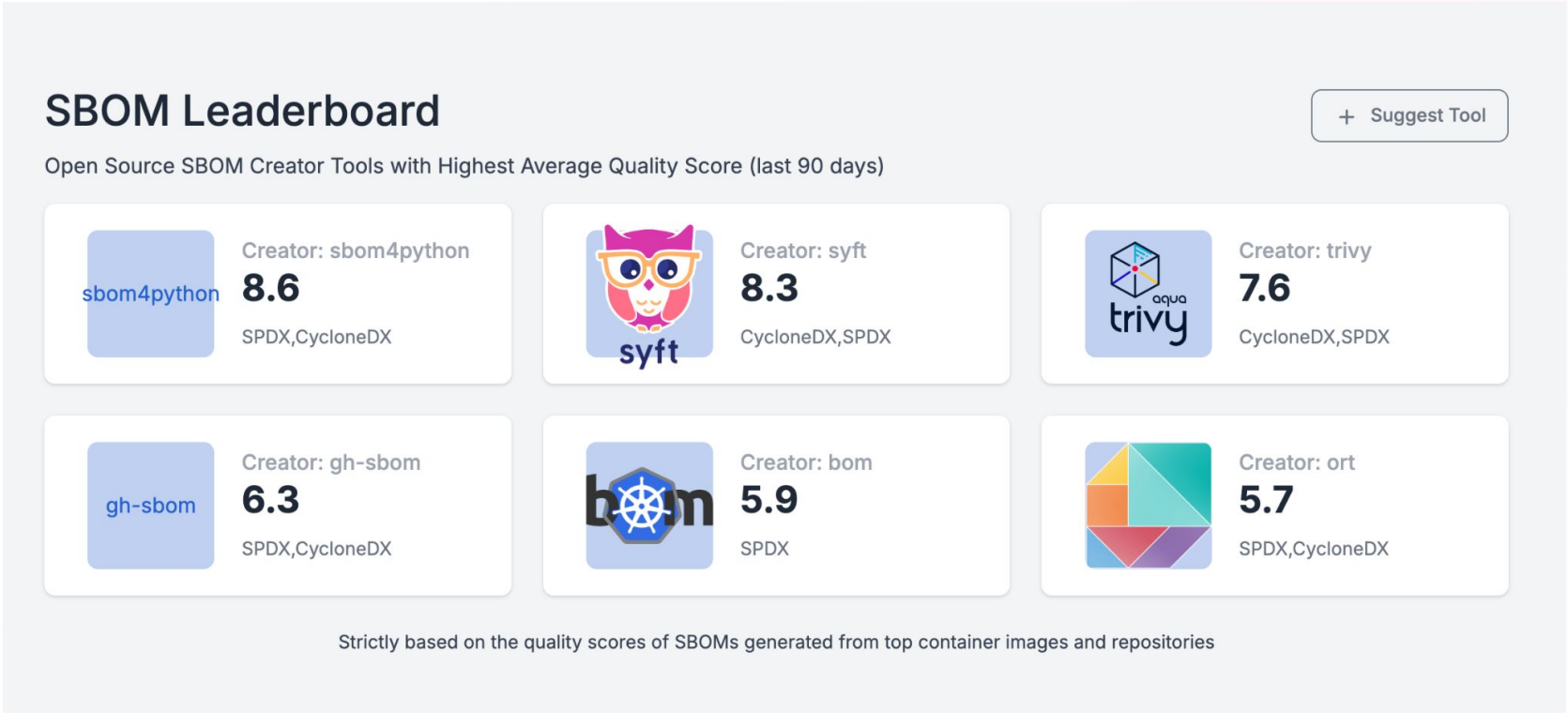
Типы:
https://github.com/package-url/purl-spec/blob/master/PURL-TYPES.rst

# Syft

- Works seamlessly with Grype (a fast, modern vulnerability scanner)
- Able to create signed SBOM attestations using the in-toto specification
- Convert between SBOM formats, such as CycloneDX, SPDX, and Syft's own format.

https://github.com/anchore/syft

# SBOM Benchmark




https://sbombenchmark.dev/

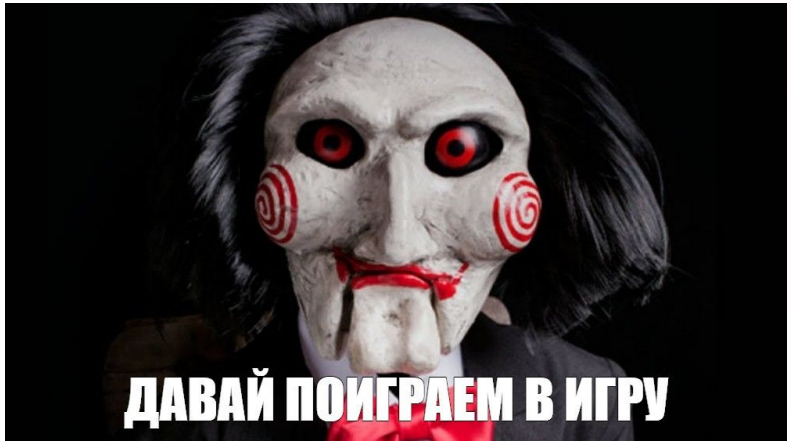
# “Компоненты” сканера

Какая-то логика получения списка ПО - версия

Компараторы версий / поиск по данным уязвимостей

*Понять уязвим ли наш пакет/ПО, конкретная версия*

# Компараторы версий



# Компараторы версий

*Что больше?*

*1-A 9.5.5*

*1-B 9.6.5*

# Компараторы версий

*Что больше?*

| | | | |
|---|---|---|---|
| *1-A* | *9.5.5* | *1-B* | *9.5.5* |
| *2-A* | ***final*** | *2-B* | ***rel01*** |

# Если вы думаете, что я в бреду...

| | id [PK] text | name text | version text |
|---|---|---|---|
| 1 | pkg:pypi/18-e@final | 18-e | final |
| 2 | pkg:pypi/accost@dev | Accost | dev |
| 3 | pkg:pypi/milla@tip | Milla | tip |
| 4 | pkg:pypi/backdoor@all | BackDoor | all |
| 5 | pkg:pypi/citebib@dev | CiteBib | dev |
| 6 | pkg:pypi/flask-markdown@dev | Flask-Markdown | dev |
| 7 | pkg:pypi/pymodelica@trunk | PyModelica | trunk |
| 8 | pkg:pypi/sirious@dev | Sirious | dev |
| 9 | pkg:pypi/pyoptimica@trunk | PyOptimica | trunk |
| 10 | pkg:pypi/taarifaapi@dev | TaarifaAPI | dev |
| 11 | pkg:pypi/bernd@leatherbill | bernd | leatherbill |
| 12 | pkg:pypi/aptdaemon@trunk | aptdaemon | trunk |
| 13 | pkg:pypi/amoi@lol | amoi | lol |
| 14 | pkg:pypi/work@dev | Work | dev |
| 15 | pkg:pypi/aa@aa | aa | aa |
| 16 | pkg:pypi/appwsgi@default | appwsgi | default |
| 17 | pkg:pypi/btb@dev | btb | dev |
| 18 | pkg:pypi/bosun@dev | bosun | dev |
| 19 | pkg:pypi/gevent-engineio@dev | gevent-engineio | dev |
| 20 | pkg:pypi/django-gmapsfield@alpha | django_gmapsfield | alpha |

# Компараторы версий

*Что больше?*

| | | | |
|---|---|---|---|
| *1-A* | *9.5.5* | *1-B* | *9.5.5* |
| *2-A* | *final* | *2-B* | *rel01* |
| *3-A* | ***1:7.2-40.4.el2.i386*** | *3-B* | ***0:7.6-40.4.el5.i386*** |

# “Компоненты” сканера

Какая-то логика получения списка ПО - версия

Компараторы версий / поиск по данным уязвимостей

Данные об уязвимостях

*что именно уязвимо и где фикс*

# Advisory database sources

Docker Scout aggregates vulnerability data from multiple sources. The data is continuously updated to ensure that your security posture is represented using the latest available information, in real-time.

Docker Scout uses the following package repositories and security trackers:

- Alpine secdb
- AlmaLinux Security Advisory
- Amazon Linux Security Center
- Bitnami Vulnerability Database
- CISA Known Exploited Vulnerability Catalog
- CISA Vulnrichment
- Debian Security Bug Tracker
- Exploit Prediction Scoring System (EPSS)
- GitHub Advisory Database
- GitLab Advisory Database
- Golang VulnDB
- inTheWild, a community-driven open database of vulnerability exploitation
- National Vulnerability Database
- Oracle Linux Security
- Python Packaging Advisory Database
- RedHat Security Data
- Rocky Linux Security Advisory
- RustSec Advisory Database
- SUSE Security CVRF
- Ubuntu CVE Tracker
- Wolfi Security Feed
- Chainguard Security Feed

https://docs.docker.com/scout/deep-dive/advisory-db-sources/

# OS

| OS | Source |
|---|---|
| Arch Linux | Vulnerable Issues |
| Alpine Linux | secdb |
| Amazon Linux 1 | Amazon Linux Security Center |
| Amazon Linux 2 | Amazon Linux Security Center |
| Debian | Security Bug Tracker |
| | OVAL |
| Ubuntu | Ubuntu CVE Tracker |
| RHEL/CentOS | OVAL |
| | Security Data |
| Oracle Linux | OVAL |
| OpenSUSE/SLES | CVRF |

# Programming Language

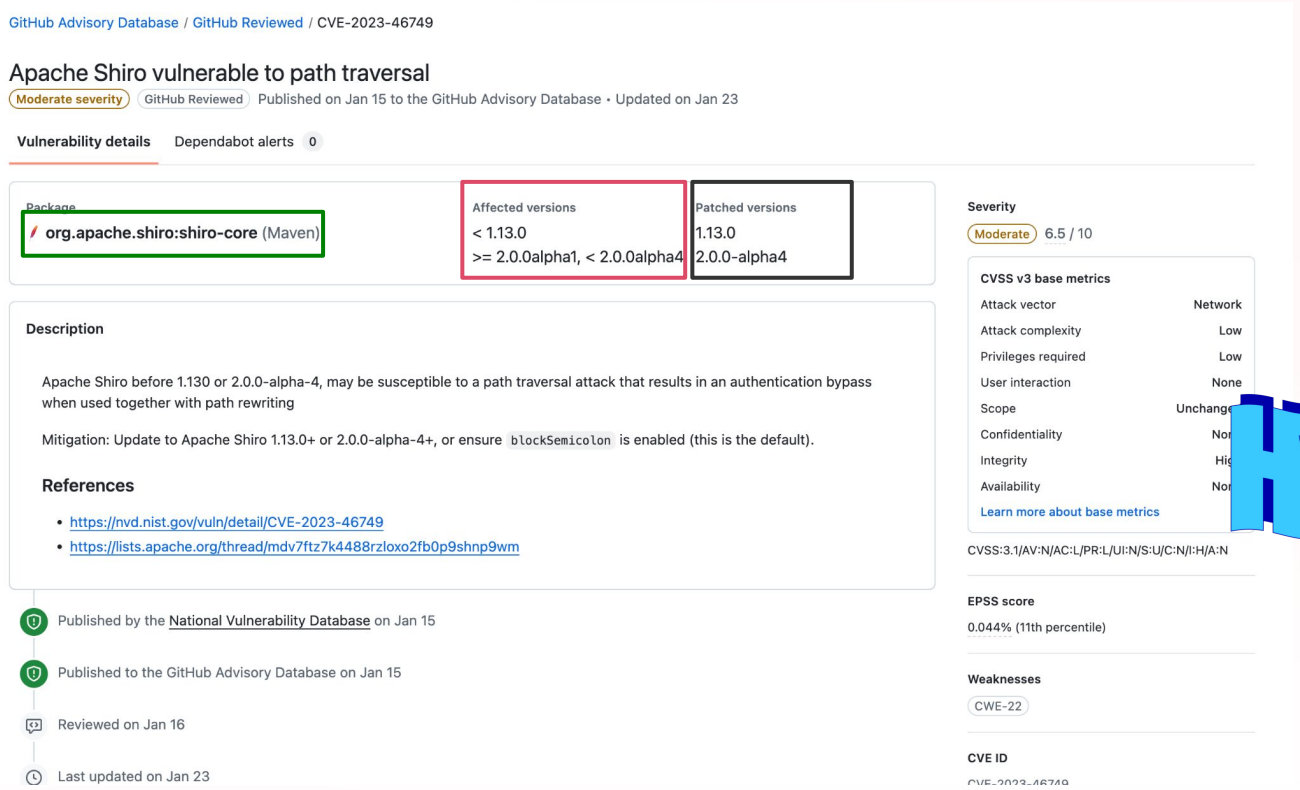
| Language | Source | Commercial Use | Delay[1] |
|---|---|---|---|
| PHP | PHP Security Advisories Database | ✅ | - |
| | GitHub Advisory Database (Composer) | ✅ | - |
| Python | Safety DB | ❌ | 1 month |
| | GitHub Advisory Database (pip) | ✅ | - |
| Ruby | Ruby Advisory Database | ❌ (partially) | - |
| | GitHub Advisory Database (RubyGems) | ✅ | - |
| Node.js | Ecosystem Security Working Group | ✅ | - |
| | GitHub Advisory Database (npm) | ✅ | - |
| Java | GitLab Advisories Community | ✅ | 1 month |
| | GitHub Advisory Database (Maven) | ✅ | - |

https://aquasecurity.github.io/trivy/v0.19.2/vulnerability/detection/data-source/

# Данные: Github Advisory

| advisory_id<br>text | first_patched_version<br>text | package_name<br>text | package_manager<br>text | version_range<br>text | severity<br>text | u<br>ti |
|---|---|---|---|---|---|---|
| GHSA-4j6x-w426-6rc6 | 0.11.17 | @cubejs-backend/api-gateway | NPM | >= 0.11.0, <= 0.11.16 | HIGH | 2 |
| GHSA-6r58-4xgr-gm6… | 4.4.4 | silverstripe/framework | COMPOSER | >= 4.4.0, < 4.4.4 | LOW | 2 |
| GHSA-89ch-hqf9-rgp3 | 2.3.3 | magento/community-edition | COMPOSER | >= 2.3, < 2.3.3 | HIGH | 2 |
| GHSA-89ch-hqf9-rgp3 | 2.2.10 | magento/community-edition | COMPOSER | >= 2.2, < 2.2.10 | HIGH | 2 |
| GHSA-f884-gm86-cg… | 3.4.1 | prestashop/ps_facetedsearch | COMPOSER | < 3.4.1 | HIGH | 2 |
| GHSA-wqq8-mqj9-69… | 4.10.1 | prestashop/autoupgrade | COMPOSER | >= 4.0.0, < 4.10.1 | HIGH | 2 |
| GHSA-769f-539v-f5jg | 2.3.2 | prestashop/gamification | COMPOSER | < 2.3.2 | HIGH | 2 |
| GHSA-r679-m633-g7… | 1.4.2 | org.apache.shiro:shiro-core | MAVEN | < 1.4.2 | HIGH | 2 |
| GHSA-9r27-994c-4xch | 2.3.1 | discord-markdown | NPM | < 2.3.1 | HIGH | 2 |
| GHSA-ff5x-w9wg-h275 | 0.2.2 | vp-toolkit | NPM | < 0.2.2 | HIGH | 2 |
| GHSA-p94w-42g3-f7… | 0.2.2 | vp-toolkit | NPM | < 0.2.2 | HIGH | 2 |
| GHSA-6hqm-866r-3civ | 3.2.2 | commons-collections:commons-collections | MAVEN | < 3.2.2 | HIGH | 2 |

# Данные: Github Advisory



GitHub Advisory Database / GitHub Reviewed / CVE-2023-46749

## Apache Shiro vulnerable to path traversal

Moderate severity | GitHub Reviewed | Published on Jan 15 to the GitHub Advisory Database • Updated on Jan 23

Vulnerability details | Dependabot alerts 0

| Package | Affected versions | Patched versions |
|---|---|---|
| org.apache.shiro:shiro-core (Maven) | < 1.13.0<br>>= 2.0.0alpha1, < 2.0.0alpha4 | 1.13.0<br>2.0.0-alpha4 |

**Description**

Apache Shiro before 1.130 or 2.0.0-alpha-4, may be susceptible to a path traversal attack that results in an authentication bypass when used together with path rewriting

Mitigation: Update to Apache Shiro 1.13.0+ or 2.0.0-alpha-4+, or ensure `blockSemicolon` is enabled (this is the default).

**References**

- https://nvd.nist.gov/vuln/detail/CVE-2023-46749
- https://lists.apache.org/thread/mdv7ftz7k4488rzloxo2fb0p9shnp9wm

Published by the National Vulnerability Database on Jan 15

Published to the GitHub Advisory Database on Jan 15

Reviewed on Jan 16

Last updated on Jan 23

**Severity**

Moderate 6.5 / 10

**CVSS v3 base metrics**

| | |
|---|---|
| Attack vector | Network |
| Attack complexity | Low |
| Privileges required | Low |
| User interaction | None |
| Scope | Unchange |
| Confidentiality | No |
| Integrity | Hi |
| Availability | No |

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N

**EPSS score**

0.044% (11th percentile)

**Weaknesses**

CWE-22

**CVE ID**

CVE-2023-46749


https://github.com/advisories/GHSA-jc7h-c423-mpjc

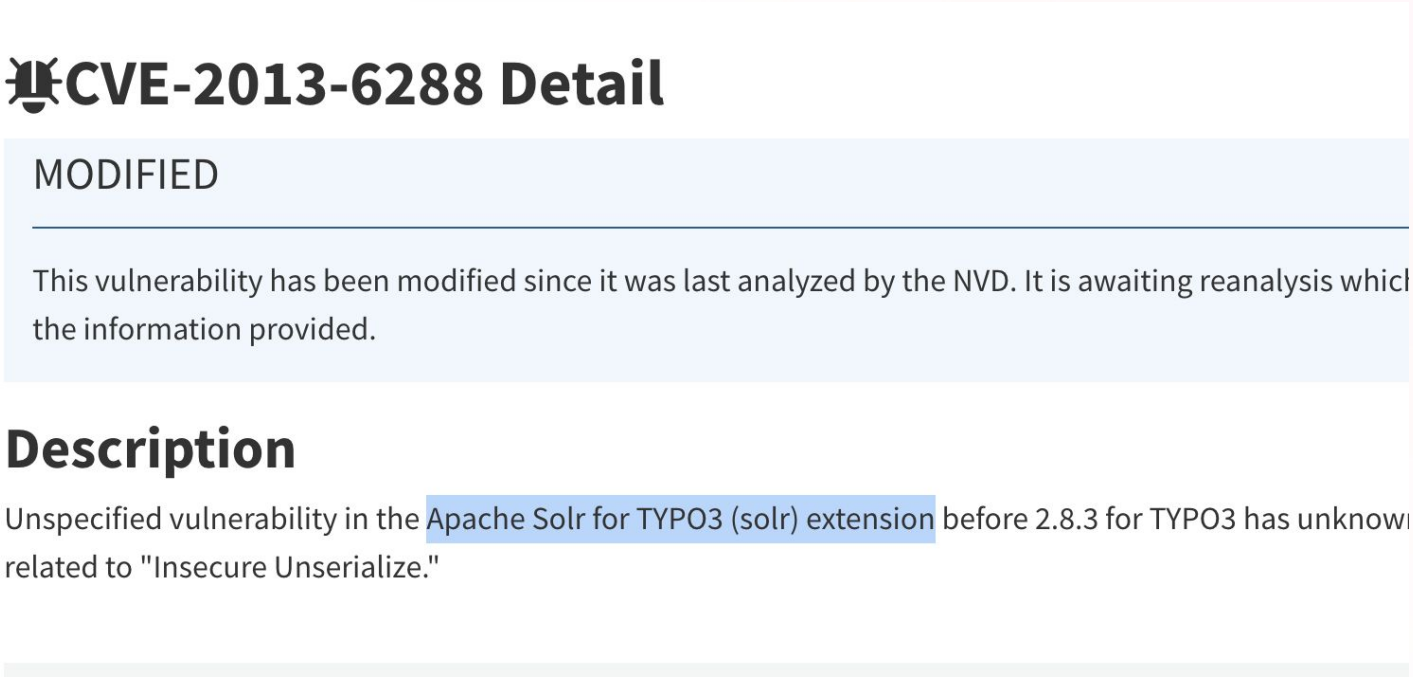
# **CPE** (Common Platform Enumeration)

| | |
|---|---|
| cpe:2.3:a:ingo_renner:apache_solr:2.1.0:*:*:*:*:*:*:* | CVE-2013-6288 |
| cpe:2.3:a:ingo_renner:apache_solr:2.2.2:*:*:*:*:*:*:* | CVE-2013-6288 |
| cpe:2.3:a:ingo_renner:apache_solr:2.8.0:*:*:*:*:*:*:* | CVE-2013-6288 |
| cpe:2.3:a:ingo_renner:apache_solr:2.8.1:*:*:*:*:*:*:* | CVE-2013-6288 |
| cpe:2.3:a:ingo_renner:apache_solr:2.8.2:*:*:*:*:*:*:* | CVE-2013-6288 |
| cpe:2.3:a:apache:solr:4.0.0:beta:*:*:*:*:*:* | CVE-2012-6612 |
| cpe:2.3:a:apache:solr:1.1.0:*:*:*:*:*:*:* | CVE-2012-6612 |
| cpe:2.3:a:apache:solr:1.2.0:*:*:*:*:*:*:* | CVE-2012-6612 |
| cpe:2.3:a:apache:solr:1.2:*:*:*:*:*:*:* | CVE-2012-6612 |
| cpe:2.3:a:apache:solr:1.3.0:*:*:*:*:*:*:* | CVE-2012-6612 |
| cpe:2.3:a:apache:solr:1.4.0:*:*:*:*:*:*:* | CVE-2012-6612 |

# **CPE** (Common Platform Enumeration)

| | |
|---|---|
| cpe:2.3:a:ingo_renner:apache_solr:2.1.0:*:*:*:*:*:*:* | CVE-2013-6288 |
| cpe:2.3:a:ingo_renner:apache_solr:2.2.2:*:*:*:*:*:*:* | CVE-2013-6288 |
| cpe:2.3:a:ingo_renner:apache_solr:2.8.0:*:*:*:*:*:*:* | CVE-2013-6288 |
| cpe:2.3:a:ingo_renner:apache_solr:2.8.1:*:*:*:*:*:*:* | CVE-2013-6288 |
| cpe:2.3:a:ingo_renner:apache_solr:2.8.2:*:*:*:*:*:*:* | CVE-2013-6288 |
| cpe:2.3:a:apache:solr:4.0.0:beta:*:*:*:*:*:* | CVE-2012-6612 |
| cpe:2.3:a:apache:solr:1.1.0:*:*:*:*:*:*:* | CVE-2012-6612 |
| cpe:2.3:a:apache:solr:1.2.0:*:*:*:*:*:*:* | CVE-2012-6612 |
| cpe:2.3:a:apache:solr:1.2:*:*:*:*:*:*:* | CVE-2012-6612 |
| cpe:2.3:a:apache:solr:1.3.0:*:*:*:*:*:*:* | CVE-2012-6612 |
| cpe:2.3:a:apache:solr:1.4.0:*:*:*:*:*:*:* | CVE-2012-6612 |

# Оказывается....



## CVE-2013-6288 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which
the information provided.

## Description

Unspecified vulnerability in the Apache Solr for TYPO3 (solr) extension before 2.8.3 for TYPO3 has unknow
related to "Insecure Unserialize."

https://nvd.nist.gov/vuln/detail/CVE-2013-6288

**NVD** - National Vulnerability Database

# T.e

**Вот это:**

```
cpe:2.3:a:ingo_renner:apache_solr:2.8.1:*:*:*:*:*:*:*
```

**На самом деле:**


https://packagist.org/packages/apache-solr-for-typo3/solr

# T.e

**Вот это:**

```
cpe:2.3:a:ingo_renner:apache_solr:2.8.1:*:*:*:*:*:*:*
```

**На самом деле:**

**apache-solr-for-typo3/**solr

```
composer require apache-solr-for-typo3/solr
```

*Apache Solr for TYPO3*

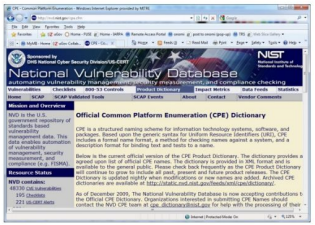
https://packagist.org/packages/apache-solr-for-typo3/solr

# 2011 год - спецификация 2.3

## How Does CPE Solve the Problem?

cpe.mitre.org

NIST NVD




CPE Dictionary

Approved names

Published names

CPE Adopters

35K+ CPE Names
Oct 2011

Proposed new names

CPE Community

Adoption Drives Success

Products

Page 5

https://cpe.mitre.org/specification/CPE_2.3_for_ITSAC_Nov2011.pdf

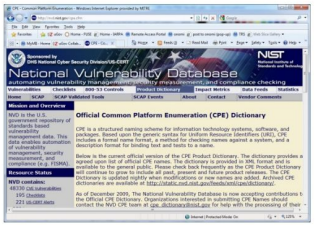
# 2011 год - спецификация 2.3



## How Does CPE Solve the Problem?

cpe.mitre.org

NIST NVD




CPE Dictionary

Approved names

Published names

35K+ CPE Names
Oct 2011

CPE Adopters

Proposed new names

CPE Community

**Adoption Drives Success**

Products

Page 5

https://cpe.mitre.org/specification/CPE_2.3_for_ITSAC_Nov2011.pdf

# CPE Dictionary

## CPE Summary

Return to Search Listing

## CPE Names

Version 2.3: **cpe:2.3:a:ingo_renner:apache_solr:1.0:*:*:*:*:*:*:***

Version 2.2: **cpe:/a:ingo_renner:apache_solr:1.0**

Read information about CPE Name encoding

### QUICK INFO

**Created On:** 10/29/2013
**Last Modified On:** 11/12/2013

### CPE NAME COMPONENTS SELECT A COMPONENT TO SEARCH FOR SIMILAR CPES

**Part:** a
**Vendor:** ingo_renner
**Product:** apache_solr
**Version:** 1.0

## Metadata

**Titles:**

| Text | Locale |
|---|---|
| Ingo Renner Apache Solr 1.0 for TYPO3 | en_US |

**References:**

| Type | Description | URL |
|---|---|---|
| | Version information | https://metrics.typo3.org/dashboard/index/org.typo3:extension-solr# |

# CPE Spec

**2011 год** - спецификация 2.3

WFNs MUST satisfy these criteria:

1. Only the following attributes SHALL be permitted in a WFN attribute-value pair:
   a. part
   b. vendor
   c. product
   d. version
   e. update
   f. edition
   g. language
   h. sw_edition
   i. target_sw
   j. target_hw
   k. other

**5.3.3.1 Part**

The *part* attribute SHALL have one of these three string values:

- The value “a”, when the WFN is for a class of applications.
- The value “o”, when the WFN is for a class of operating systems.
- The value “h”, when the WFN is for a class of hardware devices.

https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7695.pdf

# Все очень плохо

/oct 18, 2015

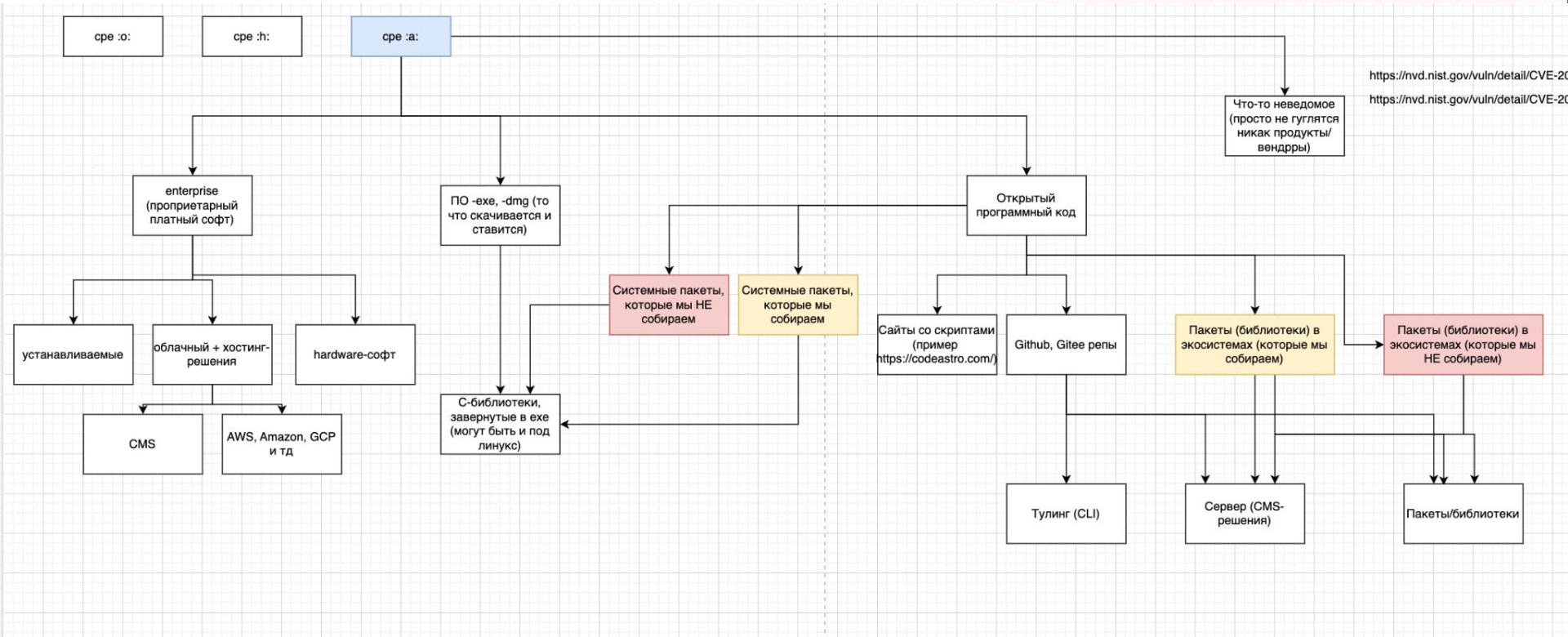
## Using CPEs for Open-Source vulnerabilities? Think Again

https://www.veracode.com/blog/managing-appsec/using-cpes-open-source-vulnerabilities-think-again

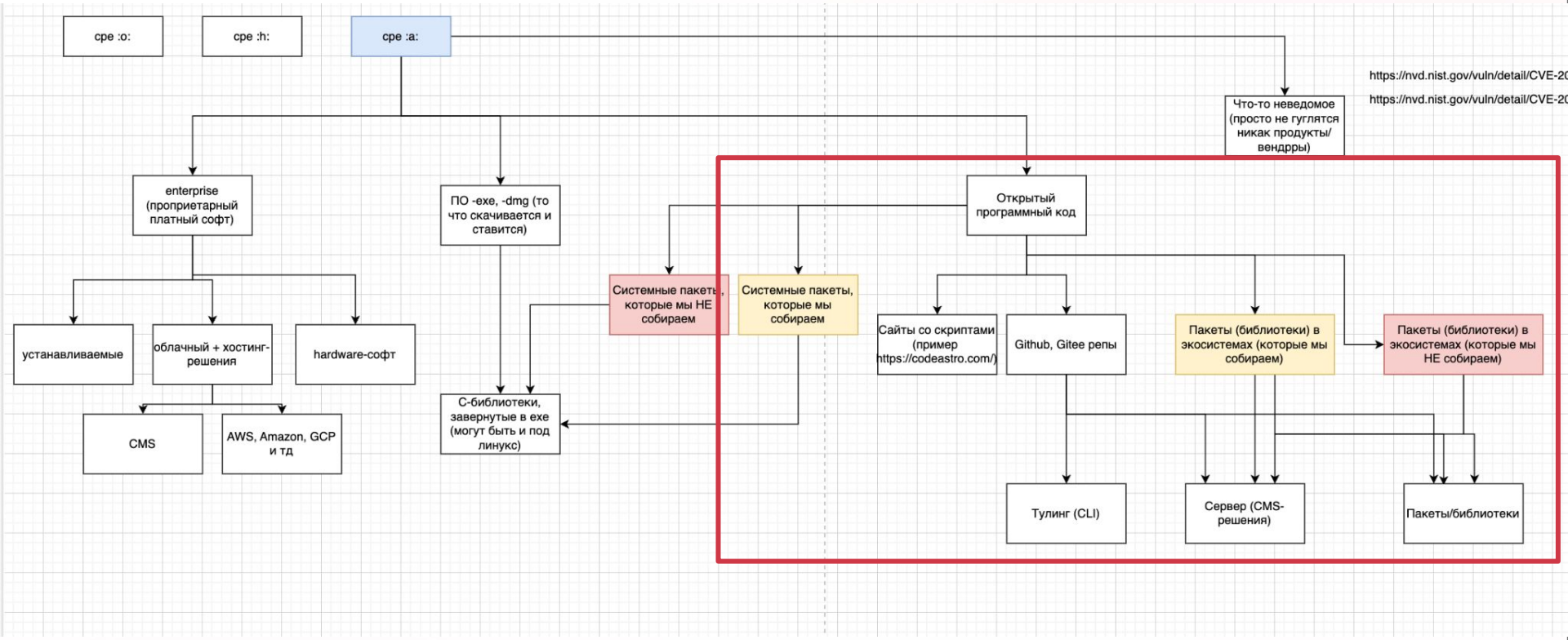
# CVE Продукты

| cve_id<br>text | product<br>text | vendor<br>text |
|---|---|---|
| CVE-2019-25214 | ShopWP | andrewmrobbins |
| CVE-2019-25215 | ARI Adminer – WordPress Database Manager | arisoft |
| CVE-2019-25216 | Rich Reviews by Starfish | starfishwp |
| CVE-2019-25217 | Speed Optimizer – The All-In-One Performance-Boosting Plugin | siteground |
| CVE-2019-25218 | Photo Gallery Slideshow & Masonry Tiled Gallery | nik00726 |
| CVE-2020-36831 | NextScripts: Social Networks Auto-Poster | nextscripts |
| CVE-2020-36832 | Indeed Membership Pro | wpindeed |
| CVE-2020-36833 | Indeed Membership Pro | wpindeed |
| CVE-2020-36834 | Discount Rules for WooCommerce – Create Smart WooCommerce Coupons & Disc… | flycart |
| CVE-2020-36835 | Migration, Backup, Staging – WPvivid | wpvividplugins |
| CVE-2020-36836 | WP Fastest Cache | emrevona |
| CVE-2020-36837 | ThemeGrill Demo Importer | themegrill |
| CVE-2020-36838 | Facebook Chat Plugin – Live Chat Plugin for WordPress | facebook |
| CVE-2020-36839 | WordPress Landing Page – Squeeze Page – Responsive Landing Page Builder Free… | bc2018 |
| CVE-2020-36840 | Timetable and Event Schedule by MotoPress | jetmonsters |

# NVD-CVE Products Types

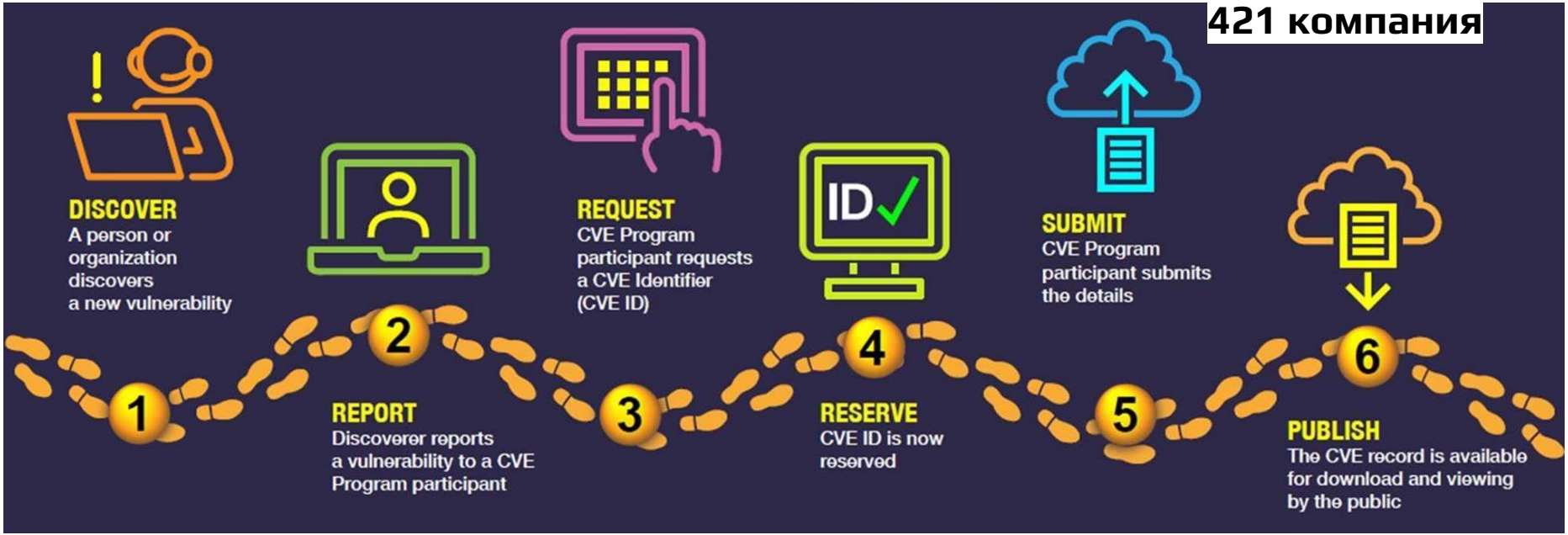


# NVD-CVE Products Types



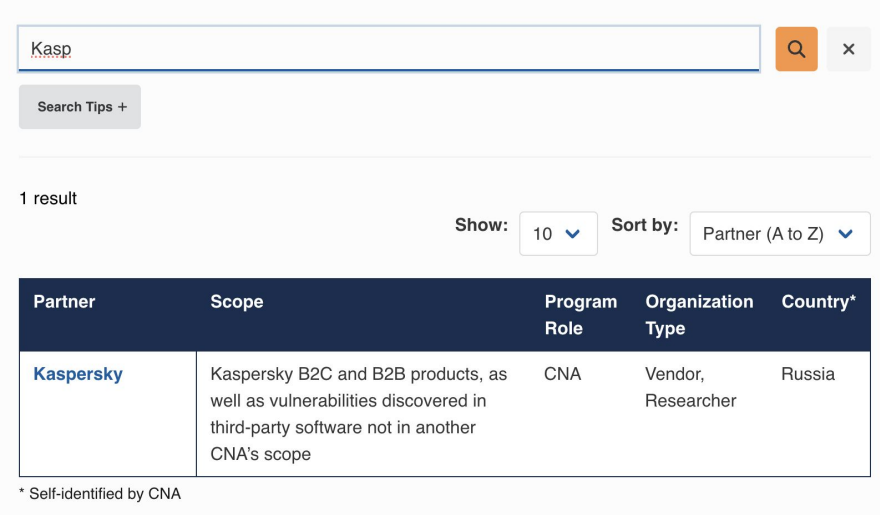
# MITRE - CVE.ORG - NVD - CPE

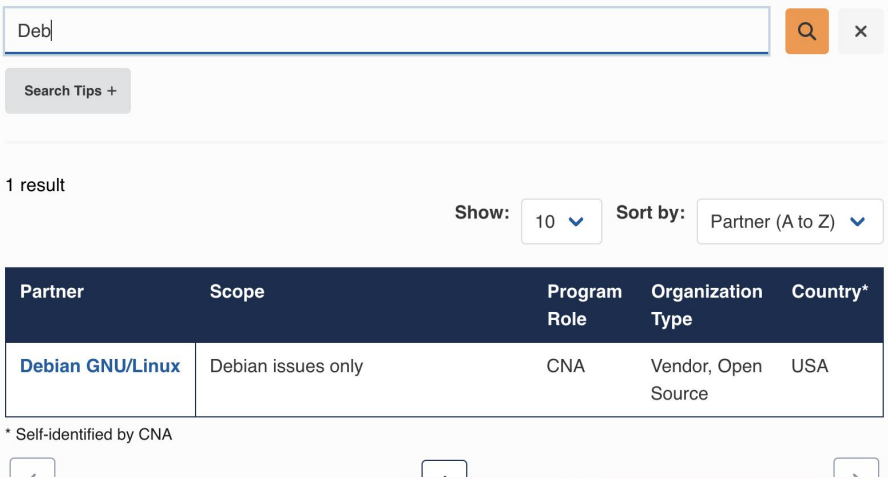
# CVE Процесс




https://www.cve.org/about/Process

# CVE Участники программы

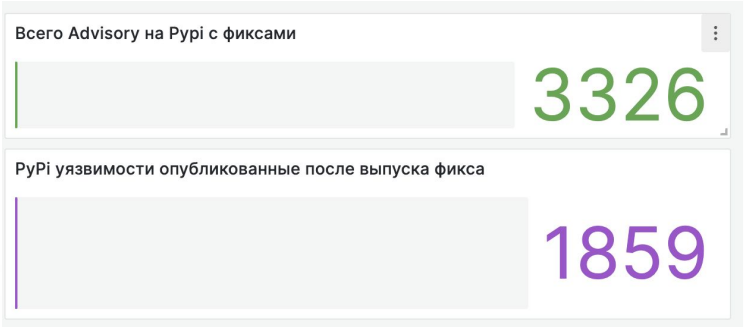


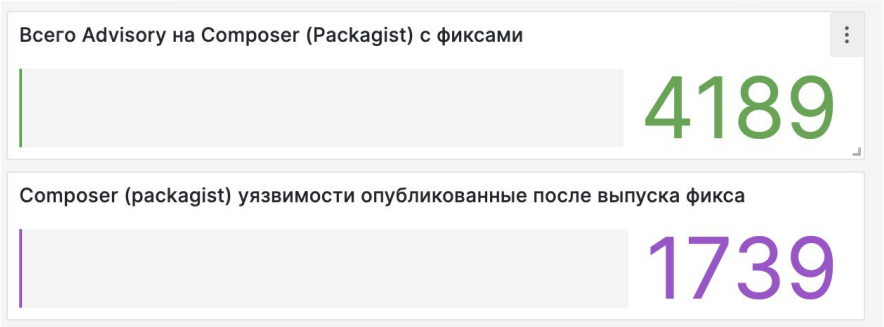

https://www.cve.org/partnerinformation/ListofPartners

# Статистика

## PyPi




## Packagist




сколько уязвимостей репортятся после выпуска фиксов по **Github Advisory**

# Где тут NVD?

## National Vulnerability Database (NVD)

CVE and NVD are separate programs. The **U.S. National Vulnerability Database (NVD)** was launched by the **National Institute of Standards and Technology (NIST)** in 2005, while the **CVE List** was launched by **The MITRE Corporation** as a community effort in 1999. The CVE List feeds NVD, which historically has built upon the information included in CVE Records to provide enhanced information for each record in its database. While separate, output from both programs is available to the public and free to use.

https://www.cve.org/about/relatedefforts

# Национальные базы уязвимостей

NVD - https://nvd.nist.gov/ (U.S. government)

BDU FSTEC - https://bdu.fstec.ru/threat (РФ)

IPA JVN iPedia - https://jvndb.jvn.jp/en/ (Япония)

CNNVD - https://www.cnvd.org.cn/ (Китай)

https://isacfoundation.org/national-security-database/ - Индия (пока нет открытой базы)

# “Кризис” NVD

скрин от
9 ноября

## CVE-2024-49195 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

### Description

Mbed TLS 3.5.x through 3.6.x before 3.6.2 has a buffer underrun in pkwrite when writing an opaque key pair

### Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

*NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.*

**CVSS 4.0 Severity and Vector Strings:**

**NIST:** NVD N/A NVD assessment not yet provided.

QUICK INFO

**CVE Dictionary Entry:**
CVE-2024-49195
**NVD Published Date:**
10/15/2024
**NVD Last Modified:**
10/17/2024
**Source:**
MITRE

### References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

| Hyperlink | Resource |
|---|---|
| https://mbed-tls.readthedocs.io/en/latest/security-advisories/mbedtls-security-advisory-2024-10-1/ | |
| https://mbed-tls.readthedocs.io/en/latest/tech-updates/security-advisories/ | |

### Weakness Enumeration

| CWE-ID | CWE Name | Source |
|---|---|---|
| CWE-787 | Out-of-bounds Write | CISA-ADP |

https://nvd.nist.gov/vuln/detail/CVE-2024-49195

# “Кризис” NVD: та же CVE на Debian

## CVE-2024-49195

debian

| | |
|---|---|
| **Name** | CVE-2024-49195 |
| **Description** | Mbed TLS 3.5.x through 3.6.x before 3.6.2 has a buffer underrun in pkwrite when writing an opaque key pair |
| **Source** | CVE (at NVD; CERT, LWN, oss-sec, fulldisc, Red Hat, Ubuntu, Gentoo, SUSE bugzilla/CVE, GitHub advisories/code/issues, web search, more) |

**Vulnerable and fixed packages**

The table below lists information on source packages.

| Source Package | Release | Version | Status |
|---|---|---|---|
| mbedtls (PTS) | bullseye | 2.16.9-0.1 | fixed |
| | bookworm | 2.28.3-1 | fixed |
| | trixie | 2.28.8-1 | vulnerable |
| | sid | 3.6.2-2 | fixed |

The information below is based on the following data on fixed versions.

| Package | Type | Release | Fixed Version | Urgency | Origin | Debian Bugs |
|---|---|---|---|---|---|---|
| mbedtls | source | bullseye | (not affected) | | | |
| mbedtls | source | bookworm | (not affected) | | | |
| mbedtls | source | (unstable) | 3.6.2-1 | | | |

https://security-tracker.debian.org/tracker/CVE-2024-49195

# Самый прикол - CISA KEV

| | | | | | |
|---|---|---|---|---|---|
| | SlimLane 29565_d74ecce0c1081d50546db573a499941b10799fb7 allows a remote attacker to escalate privileges via the PassageAutoServer.php page. | | | 48823 | |
| | Mbed TLS 3.5.x through 3.6.x before 3.6.2 has a buffer underrun in pkwrite when writing an opaque key pair | 2024-10-15 | 9.8 | CVE-2024-49195 | cve@mitre.org cve@mitre.org |
| | Buffer Overflow vulnerability in esp-idf v.5.1 allows a remote attacker to obtain sensitive information via the externalId | 2024-10-17 | 8.1 | CVE-2024-33453 | cve@mitre.org |

https://www.cisa.gov/news-events/bulletins/sb24-295

# С марта - Awaiting Analyze

## CVE-2024-28176 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

### Description

jose is JavaScript module for JSON Object Signing and Encryption, providing support for JSON Web Tokens (JWT), JSON Web Signature (JWS), JSON Web Encryption (JWE), JSON Web Key (JWK), JSON Web Key Set (JWKS), and more. A vulnerability has been identified in the JSON Web Encryption (JWE) decryption interfaces, specifically related to the support for decompressing plaintext after its decryption. Under certain conditions it is possible to have the user's environment consume unreasonable amount of CPU time or memory during JWE Decryption operations. This issue has been patched in versions 2.0.7 and 4.15.5.

### Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

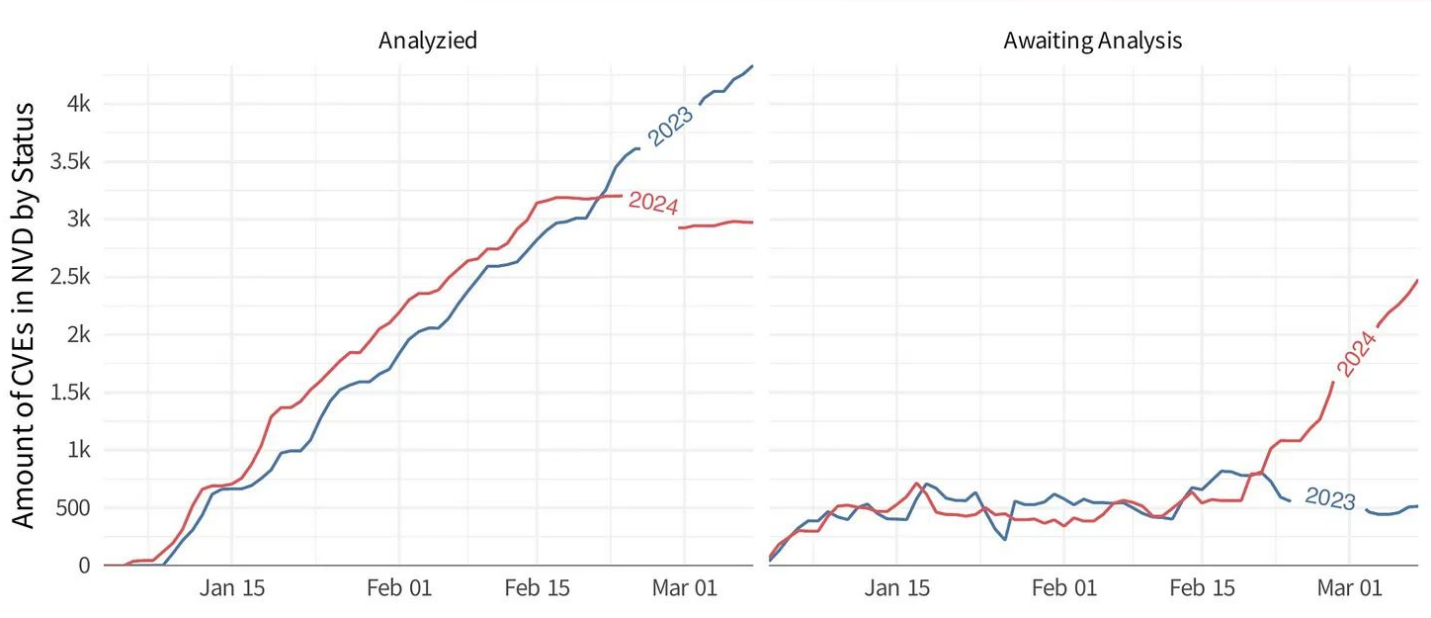
*NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.*

QUICK INFO

**CVE Dictionary Entry:**
CVE-2024-28176
**NVD Published Date:**
03/08/2024
**NVD Last Modified:**
03/30/2024
**Source:**
GitHub, Inc.

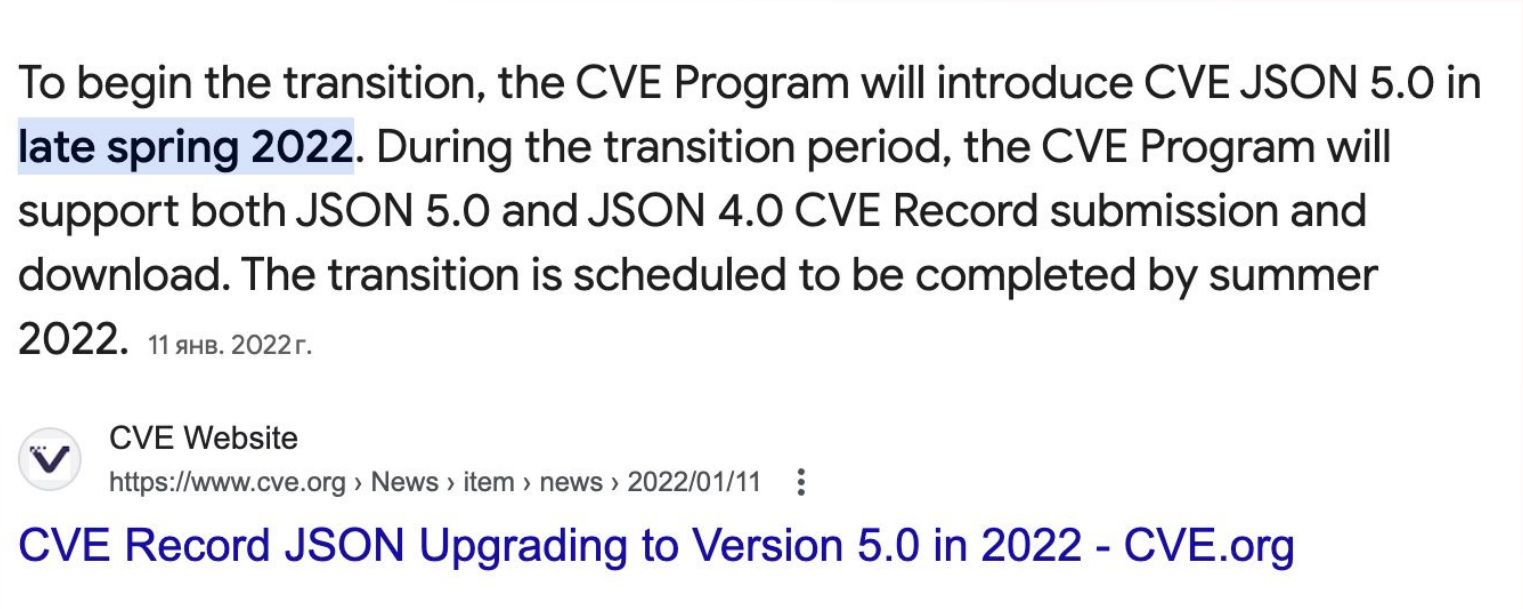
https://nvd.nist.gov/vuln/detail/CVE-2024-28176

# Дополнительно




https://www.resilientcyber.io/p/death-knell-of-the-nvd

# CVE-эволюция




https://github.com/CVEProject/cve-schema

# CVE-эволюция

## packageName в v5 спецификации

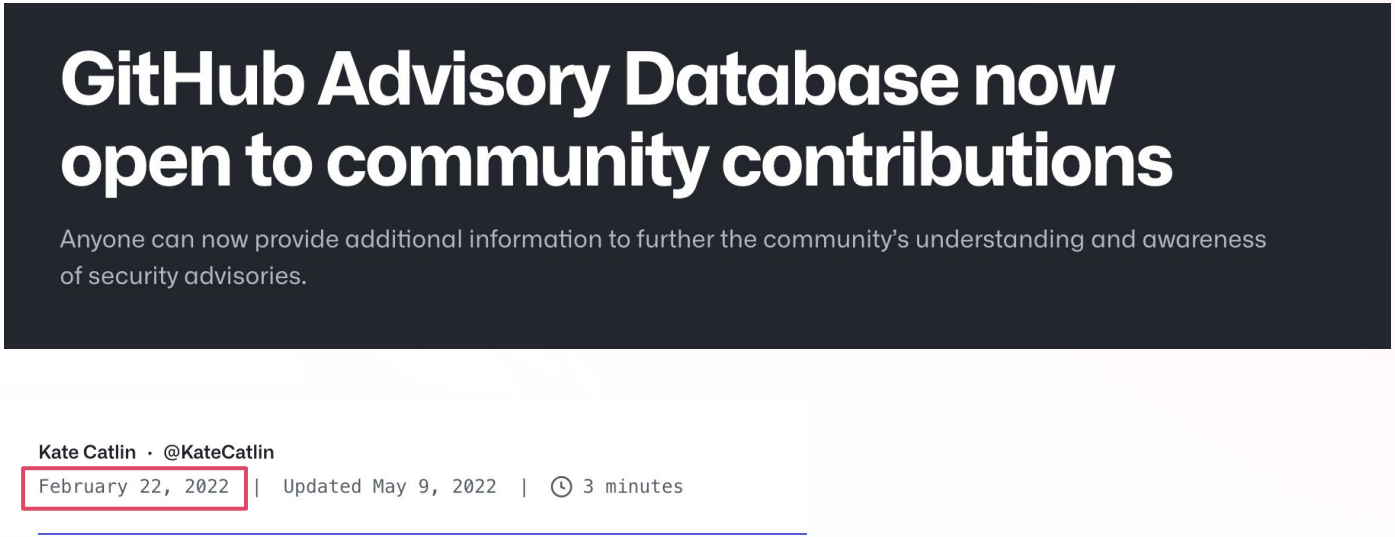
cve-schema / schema / archive / v5.0 / CVE_JSON_5.0_schema.json

```
85              "minLength": 1,
86              "maxLength": 1024
87          },
88          "status": {
89              "description": "The vulnerability status of a given version or range of versions of a product. The statuses
90              "type": "string",
91              "enum": ["affected", "unaffected", "unknown"]
92          },
93          "product": {
94              "type": "object",
95              "description": "Provides information about the set of products and services affected by this vulnerability."
96              "allOf": [
97                  {
98                      "anyOf": [
99                          {"required": ["vendor", "product"]},
100                         {"required": ["collectionURL", "packageName"]}
101                     ]
102                 },
103                 {
104                     "anyOf": [
105                         {"required": ["versions"]},
106                         {"required": ["defaultStatus"]}
107                     ]
108                 }
109             ],
110             "properties": {
111                 "vendor": {
112                     "type": "string",
```

пока правда всего в 6638 из 269076 уязвимостей

https://github.com/CVEProject/cve-schema

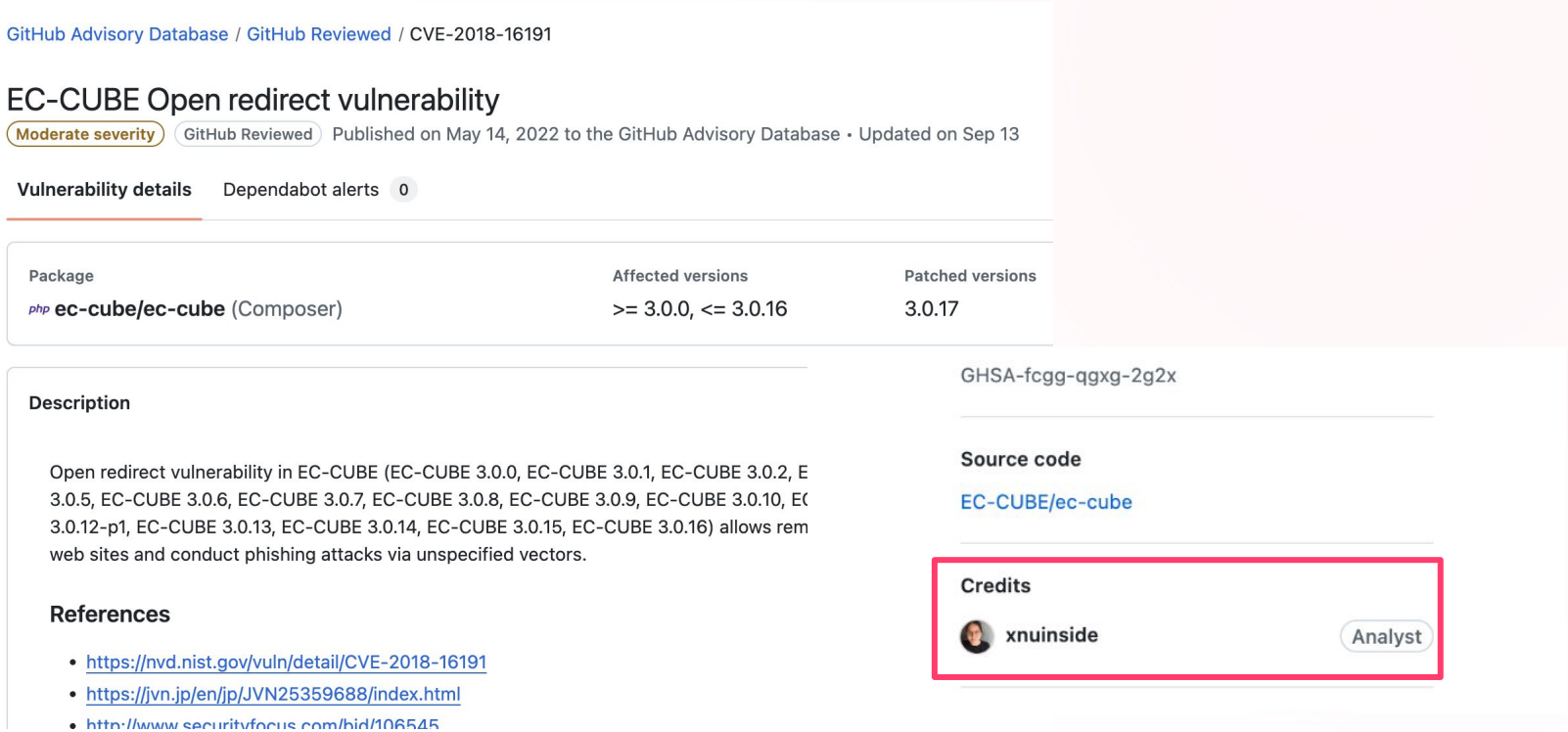
# Опенсорс, но не совсем




https://github.blog/security/vulnerability-research/github-advisory-database-now-open-to-community-contributions/

# Знаете, я и сам своего рода тоже, аналитик..

# “Аналитики” в GitHub




https://github.com/advisories/GHSA-fcgg-qgxg-2g2x

# OSV.dev

In 2021, we announced the launch of OSV, a database of open source vulnerabilities built partially from vulnerabilities found through Google's OSS-Fuzz program. OSV has grown since then and now includes a widely adopted OpenSSF schema and a vulnerability scanner. In this blog post, we'll cover how these tools help maintainers track vulnerabilities from discovery to remediation, and how to use OSV together with other SBOM and VEX standards.

https://security.googleblog.com/2023/03/osv-and-vulnerability-life-cycle.html

# **OSV Schema** (Open Source Vulnerability schema)

CODE SCORING


```
{
    "schema_version": "1.2.0",
    "id": "RUSTSEC-2019-0033",
    "published": "2019-11-16T00:00:00Z",
    "modified": "2021-01-04T19:02:00Z",
    "aliases": ["CVE-2020-25574", "CVE-2019-25008"],
    "summary": "Integer Overflow in HeaderMap::reserve() can cause Denial of Service",
    "details": "HeaderMap::reserve() used usize::next_power_of_two() to calculate\nthe increased capacity. Ho
    "references": [
      {"type": "REPORT", "url": "https://github.com/hyperium/http/issues/352"},
      {"type": "ADVISORY", "url": "https://rustsec.org/advisories/RUSTSEC-2019-0033.html"}
    ],
    "affected": [ {
        "package": {
            "ecosystem": "crates.io",
            "name": "http"
        },
        "ranges": [
            {
                "type": "SEMVER",
                "events": [
                    {"introduced": "0"},
                    {"fixed": "0.1.20"}
                ]
            }
        ],
        "ecosystem_specific": {
            "functions": ["http::header::HeaderMap::reserve"],
            "keywords": ["http", "integer-overflow", "DoS"],
            "categories": ["denial-of-service"],
            "severity": "HIGH"
        }
    } ]
}
```


https://ossf.github.io/osv-schema/#purpose

# OSV.dev


https://github.com/google/osv.dev

https://security.googleblog.com/2023/03/osv-and-vulnerability-life-cycle.html

# Языковые сканеры

`npm audit` → JS

`dotnet list package --vulnerable` → Microsoft® .NET

# Про сканеры кода

```
dotnet list package --vulnerable
```

March 2nd, 2021

## How to Scan NuGet Packages for Security Vulnerabilities

Microsoft® .NET

Today, we are announcing the public availability of NuGet's vulnerability features that you can use to ensure your projects are vulnerability free and if not, to take action to securing your software supply chain.

https://devblogs.microsoft.com/nuget/how-to-scan-nuget-packages-for-security-vulnerabilities/

# Про сканеры кода

```
dotnet list package --vulnerable
```

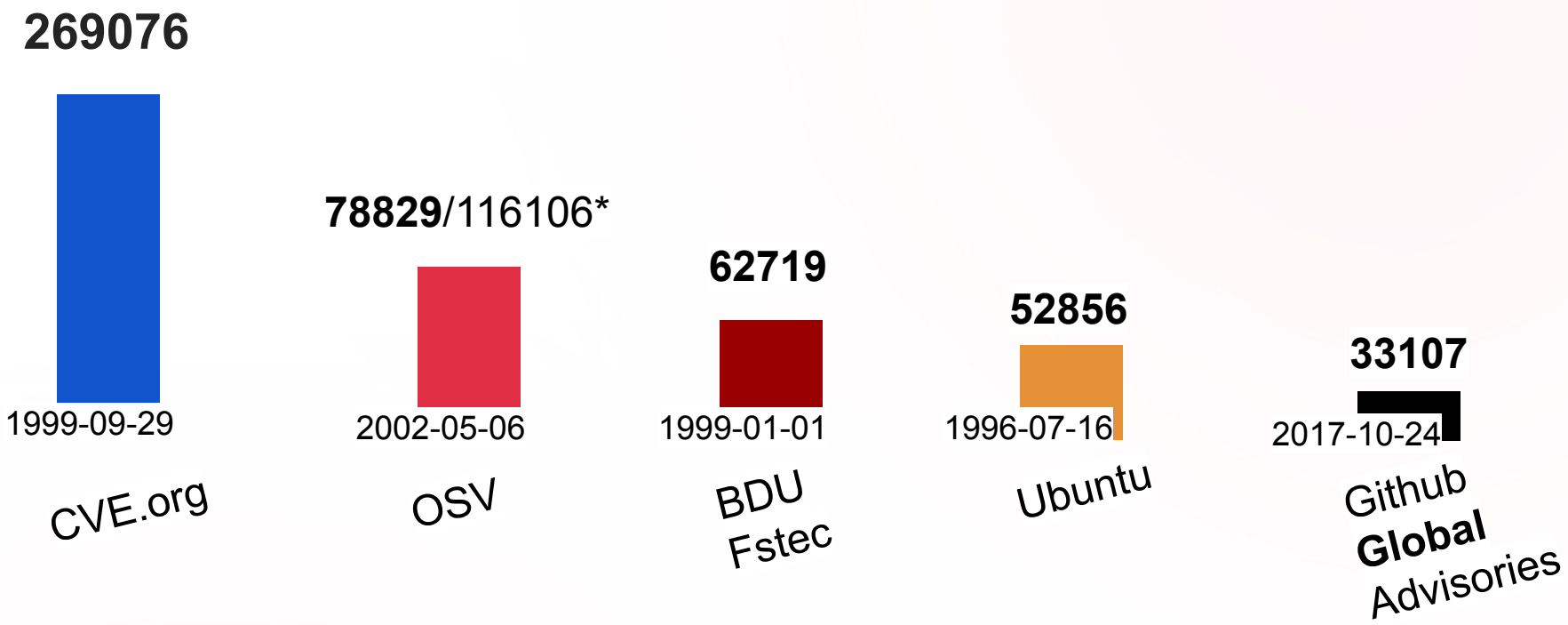

## Where do CVE/GHSA come from?

NuGet gets its CVE/GHSA information directly from the centralized GitHub Advisory Database. The database provides two main listings of vulnerabilities:

- A **CVE** is Common Vulnerabilities and Exposures. This is a list of publicly disclosed computer security flaws.

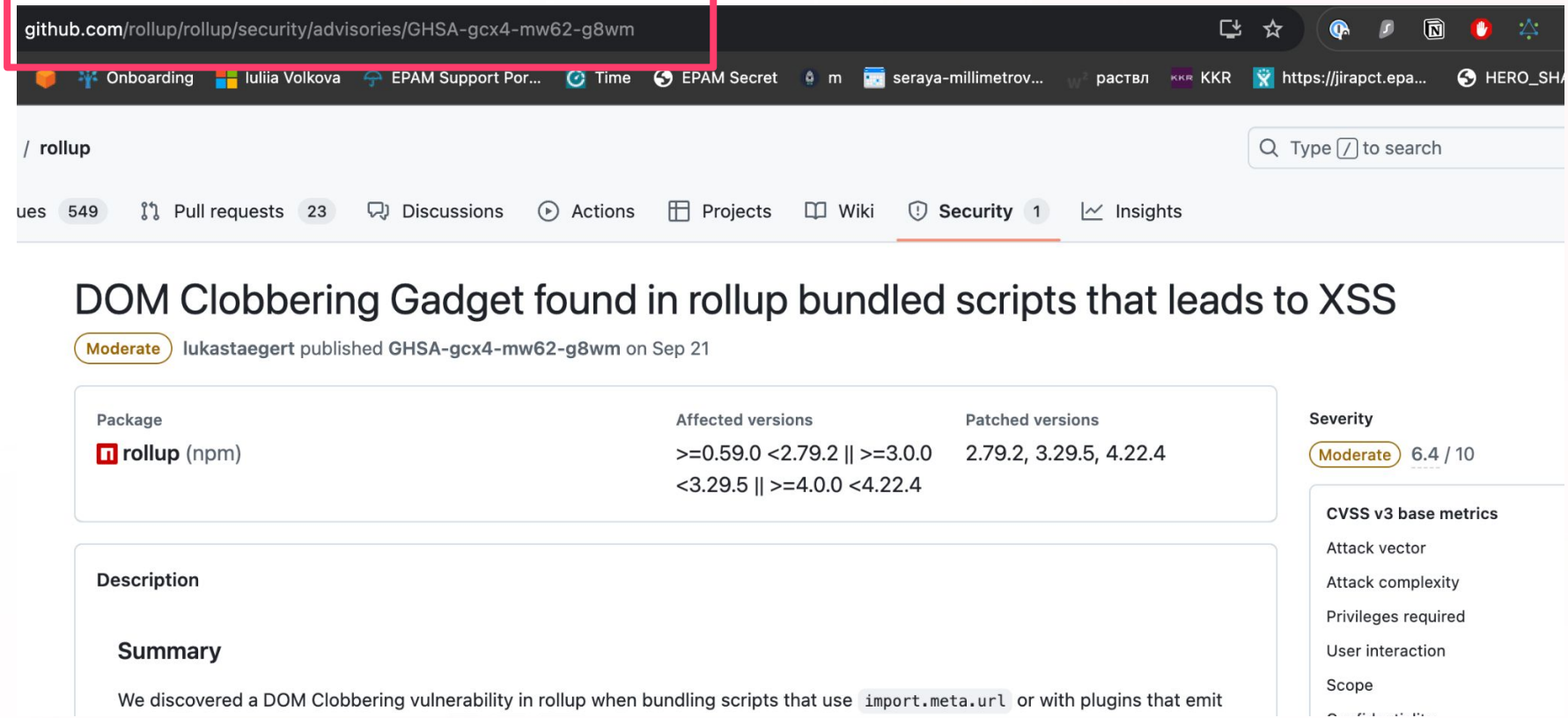
https://devblogs.microsoft.com/nuget/how-to-scan-nuget-packages-for-security-vulnerabilities/

# Немного статистики (на 12 ноября 2024)



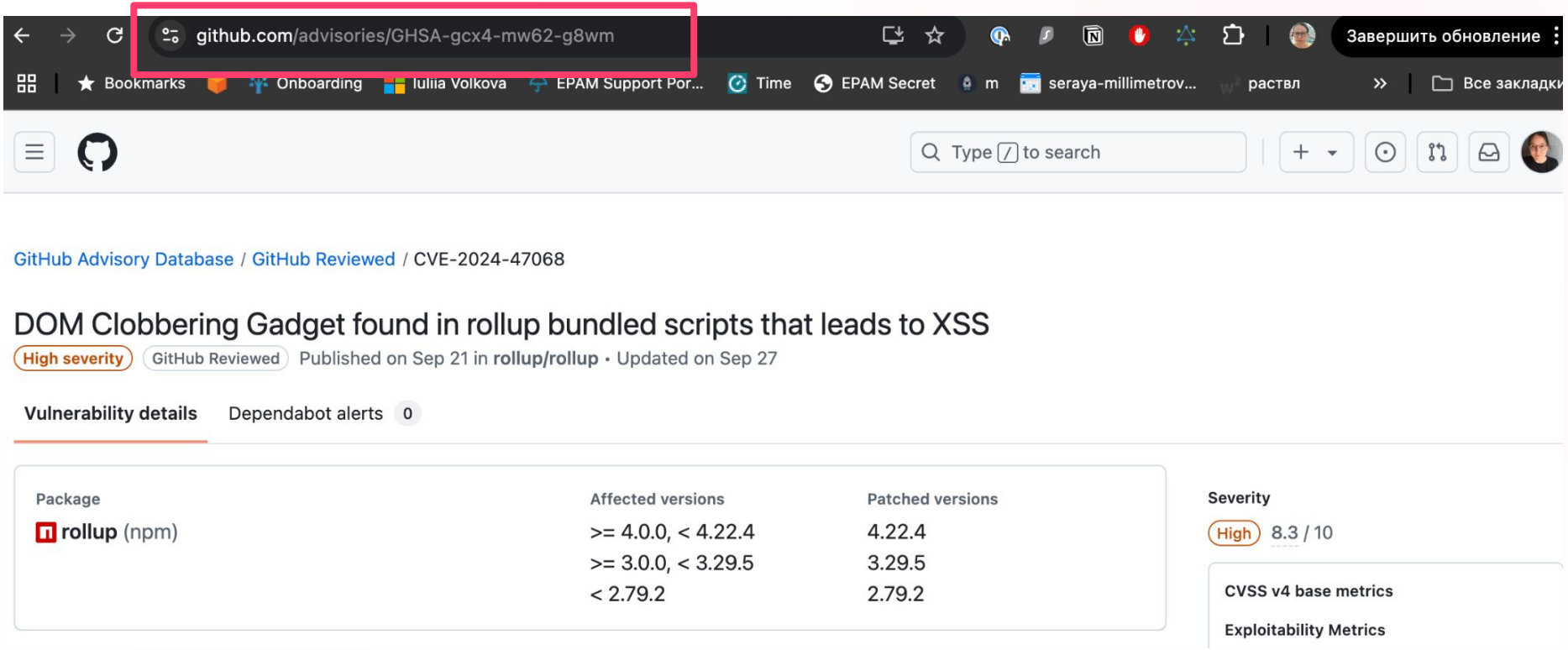

количество уязвимостей и минимальная дата уязвимости
*(для OSV) единиц информации всего, в OSV содержаться также бюллетени

# Github Repository Advisories




https://github.com/rollup/rollup/security/advisories/GHSA-gcx4-mw62-g8wm

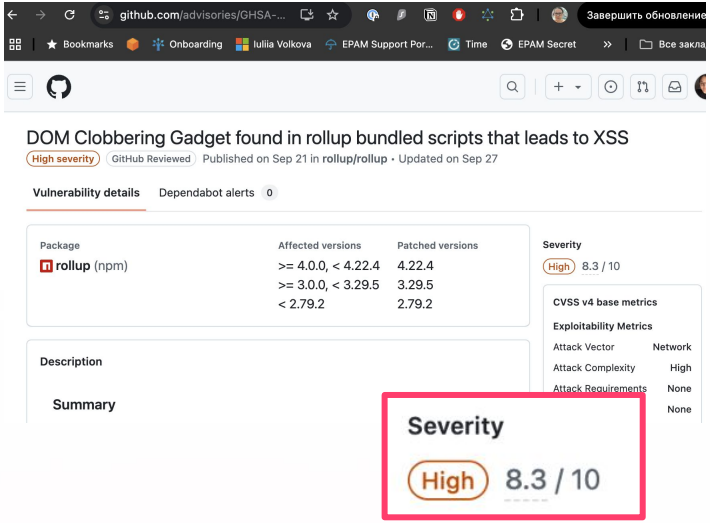
# Github Repository может дублироваться на Global Advisories



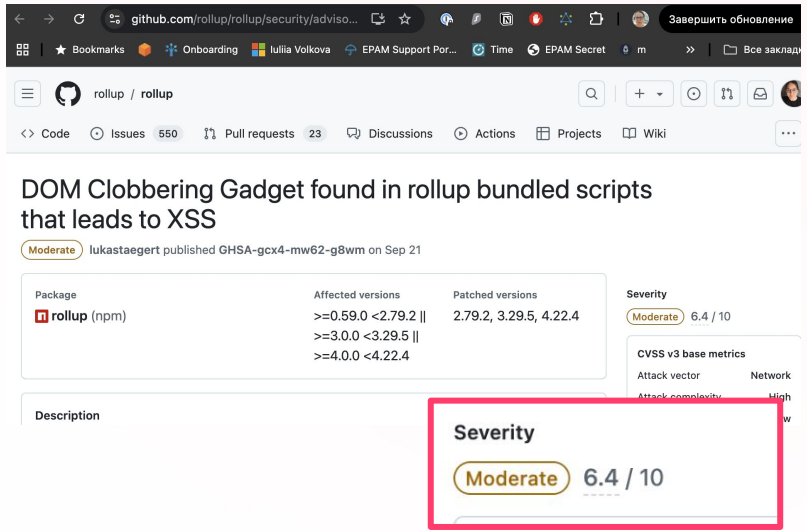

https://github.com/advisories/GHSA-gcx4-mw62-g8wm

# И могут отличаться данные

https://github.com/advisories/GHSA-gcx4-mw62-g8wm



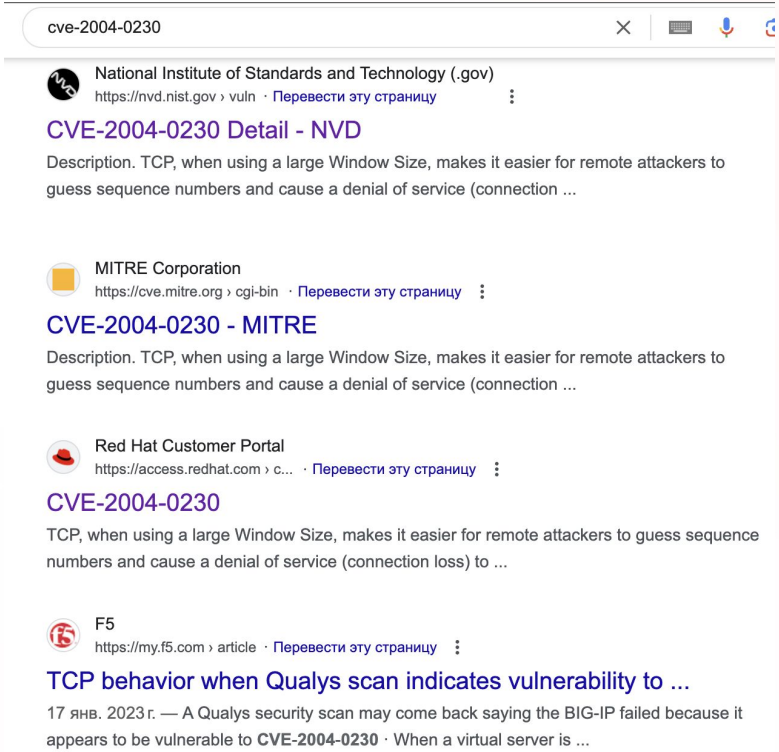

https://github.com/rollup/rollup/security/advisories/GHSA-gcx4-mw62-g8wm



# План: как искать “source” of True

если где-то
ответ “да” - то
== “фолз”

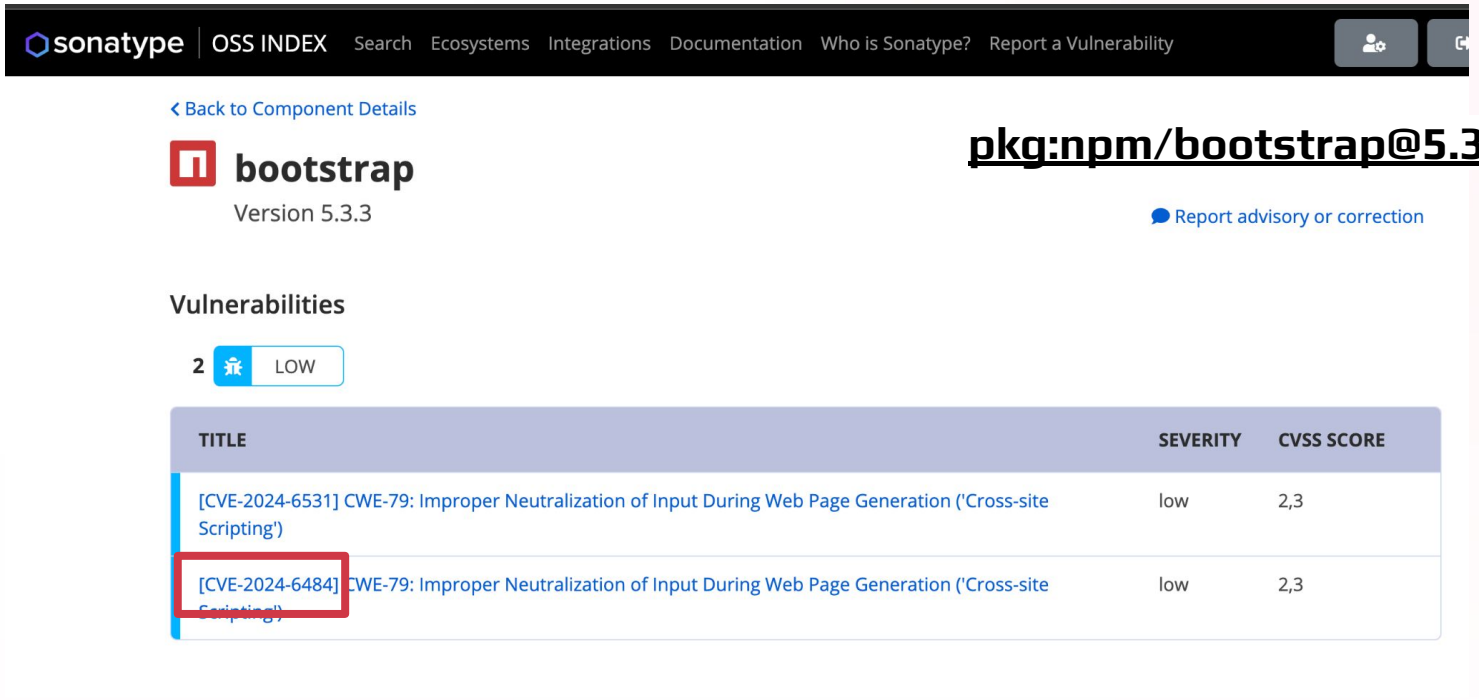
# **Шаг 1.** Вбейте в google



# Приоритет доверия


1. OS Security Trackers  (Debian, Ubuntu, и тд); CVE.org; Github Advisory (приоритет Global Advisory)
2. “Пакетные” Advisory - GoVuln DB, PyPa Advisory, RUST Sec  и тд, в том числе через OSV;
3. Gitlab Advisory (и другие менее популярные)
4. NVD
5. “Резолверы” - OSS Index, mvnrepository, и тд

# OSS Index




https://ossindex.sonatype.org/component/pkg:npm/bootstrap@5.3.3

# OSS Index

## QUICK INFO

**CVE Dictionary Entry:**
CVE-2024-6531
**NVD Published Date:**
07/11/2024
**NVD Last Modified:**
07/12/2024
**Source:**
HeroDevs

## Vulnerability Details

| | |
|---|---|
| ID | CVE-2024-6531 |
| PROJECT AFFECTED | Bootstrap |
| VERSIONS AFFECTED | >=4.0.0 <=4.6.2 |
| PUBLISHED DATE | July 11, 2024 |
| ≈ FIX DATE | July 11, 2024 |
| FIXED IN | Bootstrap NES |
| SEVERITY | Medium |
| CATEGORY | Cross-Site Scripting |

https://www.herodevs.com/vulnerability-directory/cve-2024-6531

# OSS Index

## QUICK INFO

**CVE Dictionary Entry:**
CVE-2024-6531
**NVD Published Date:**
07/11/2024
**NVD Last Modified:**
07/12/2024
**Source:**
HeroDevs

## Vulnerability Details

| | |
|---|---|
| ID | CVE-2024-6531 |
| PROJECT AFFECTED | Bootstrap |
| VERSIONS AFFECTED | >=4.0.0 <=4.6.2 |
| PUBLISHED DATE | July 11, 2024 |
| ≈ FIX DATE | July 11, 2024 |
| FIXED IN | Bootstrap NES |
| SEVERITY | Medium |
| CATEGORY | Cross-Site Scripting |

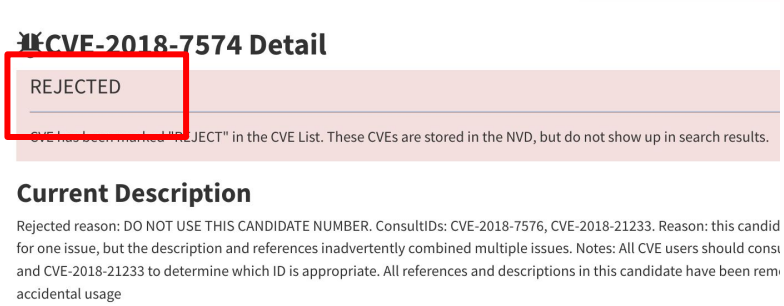
https://www.herodevs.com/vulnerability-directory/cve-2024-6531

# OSS Index in Dependency Check

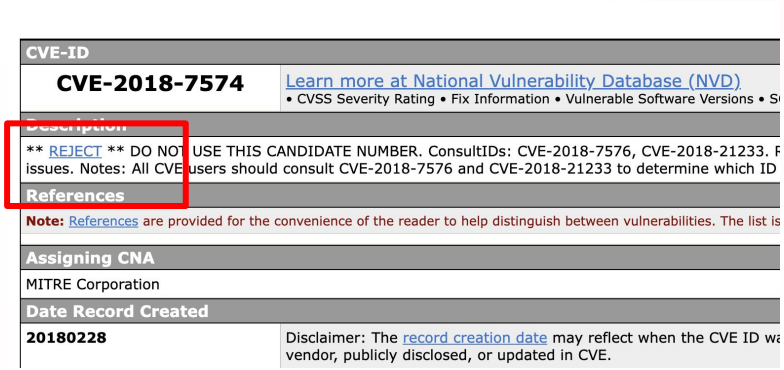
Dependency-check has a command line interface, a Maven plugin, an Ant task, and a Jenkins plugin. The core engine contains a series of analyzers that inspect the project dependencies, collect pieces of information about the dependencies (referred to as evidence within the tool). The evidence is then used to identify the Common Platform Enumeration (CPE) for the given dependency. If a CPE is identified, a listing of associated Common Vulnerability and Exposure (CVE) entries are listed in a report. Other 3rd party services and data sources such as the NPM Audit API, the OSS Index, RetireJS, and Bundler Audit are utilized for specific technologies.

https://owasp.org/www-project-dependency-check/

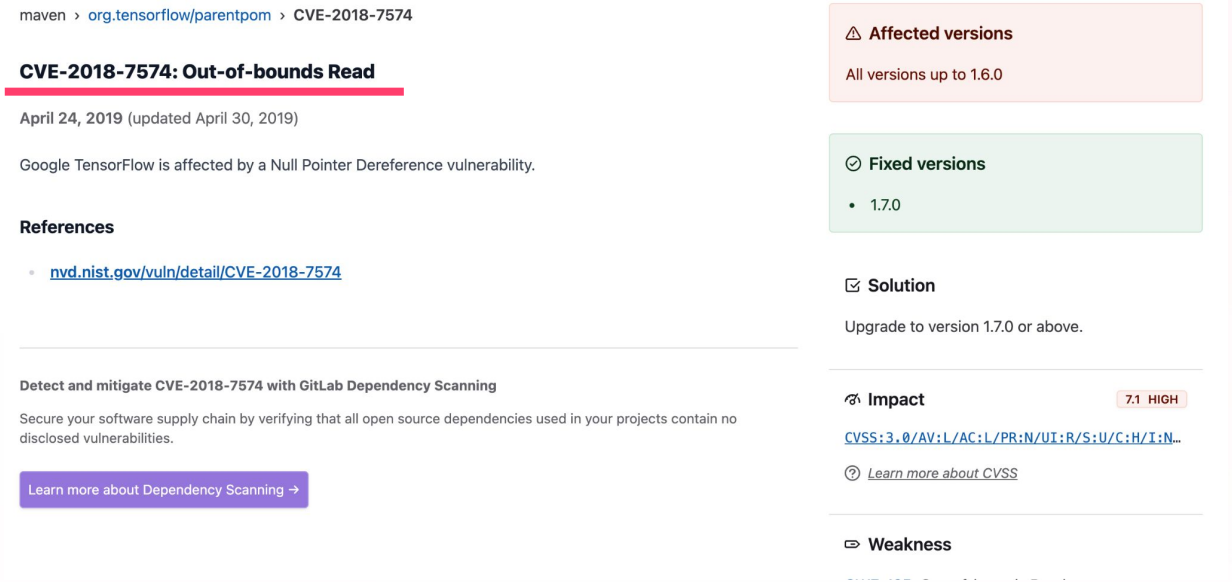
# **Шаг 2.** Отозвана ли уязвимость?



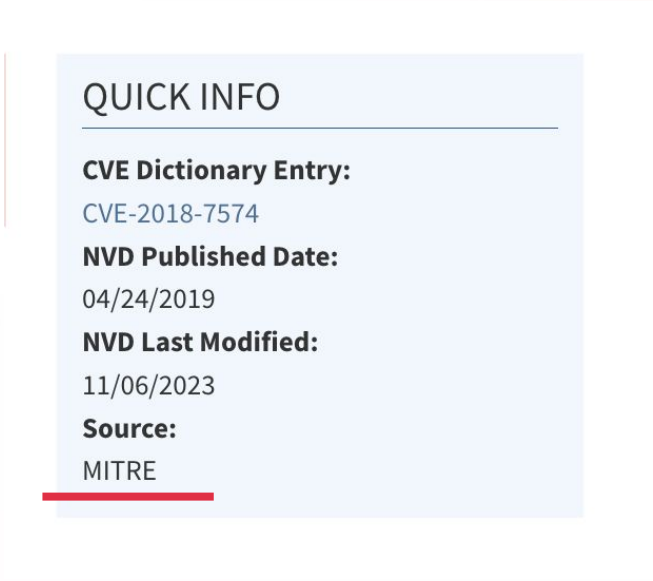




# **Шаг 2.** Но тут конечно, бывают загвоздки..



# **Шаг 2.2** При разрешении “спорных” моментов - смотрим на репортера уязвимости




всегда смотрим данные на изначальном репортере, если есть такая возможность

# **Лирика в сторону:** метрики и пакеты

## CVE-2024-47875 Detail

UNDERGOING ANALYSIS

This vulnerability is currently undergoing analysis and not all information is available. Please check back soon to view the completed vulnerability summary.

### Description

DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTML, MathML and SVG. DOMpurify was vulnerable to nesting-based mXSS. This vulnerability is fixed in 2.5.0 and 3.1.3.

QUICK INFO

**CVE Dictionary Entry:**
CVE-2024-47875
**NVD Published Date:**
10/11/2024
**NVD Last Modified:**
10/15/2024
**Source:**
GitHub, Inc.

### Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

*NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.*

**CVSS 3.x Severity and Vector Strings:**

| | | | |
|---|---|---|---|
| **NIST:** NVD | **Base Score:** N/A | NVD assessment not yet provided. | |
| **CNA:** GitHub, Inc. | **Base Score:** 10.0 CRITICAL | **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H | |

https://github.com/cure53/DOMPurify/security/advisories/GHSA-gx9m-whjm-85jf

### Weakness Enumeration

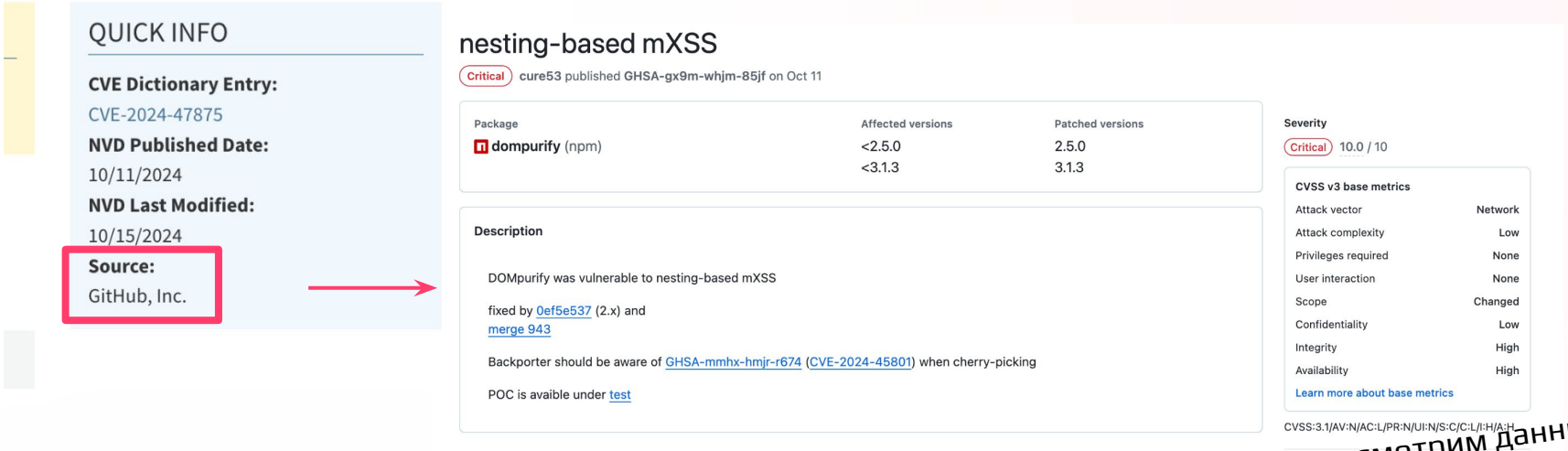
| CWE-ID | CWE Name | Source |
|---|---|---|
| CWE-79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | GitHub, Inc. |

### Change History

1 change records found show changes

https://nvd.nist.gov/vuln/detail/CVE-2024-47875

# **Лирика в сторону:** метрики и пакеты




всегда смотрим данные на изначальном репортере, если есть такая возможность

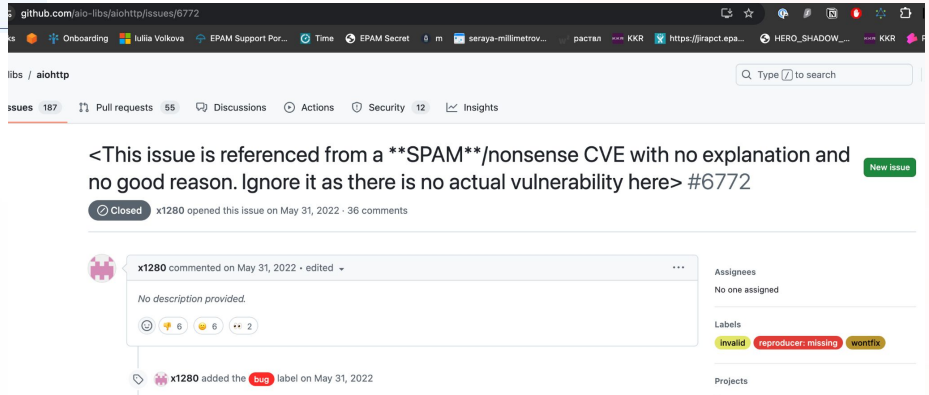
https://nvd.nist.gov/vuln/detail/CVE-2024-47875

# War 3. He disputed?

## CVE-2022-33124 Detail

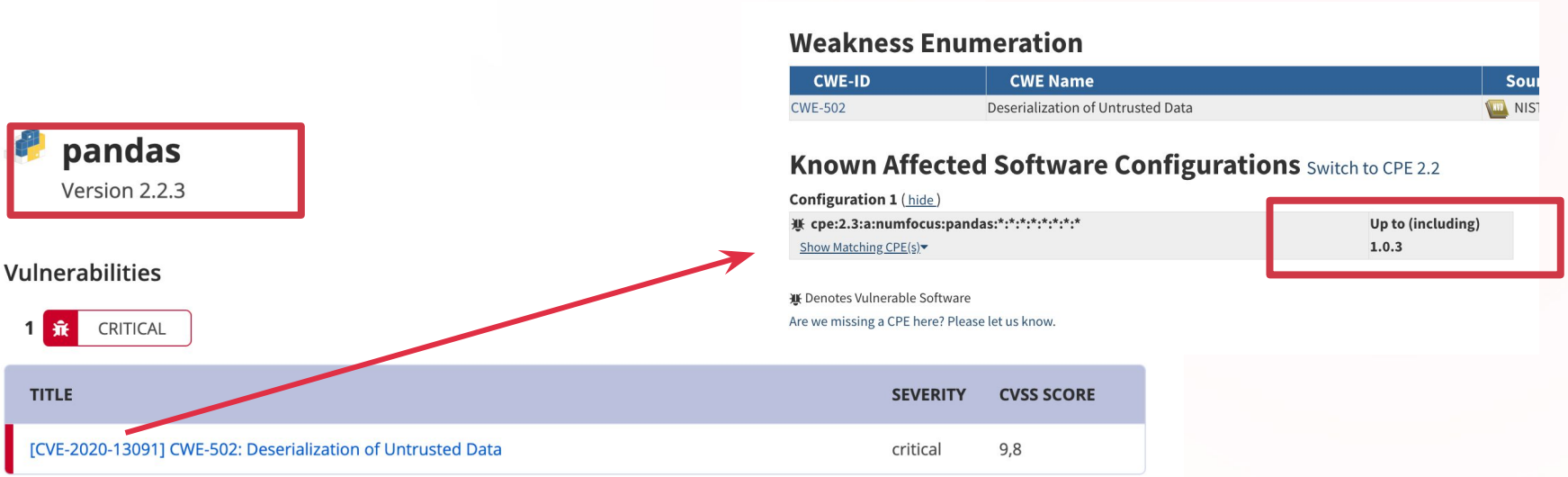
**Disputed**

MODIFIED




https://nvd.nist.gov/vuln/detail/CVE-2022-33124

# **Шаг 4.** Если fixed_version есть и есть уязвимый рейндж - внимательно смотрим на название пакета и версии




тут начинаются ошибки резолвинга (когда тула не правильно сделала “мэтч”)

# **Шаг 5.** Если fixed_version нет и нет уязвимого range

Смириться и подождать - как правило большинство тулинга считает в таких ситуациях все пакеты по умолчанию уязвимыми.

Хотя на самом деле, по спеке CVE это задается в ‘defultStatus’.

# **Шаг 5.** Если fixed_version нет и нет уязвимого range

```
                {"required": ["collectionURL", "packageN
            ]
        },
        {
            "anyOf": [
                {"required": ["versions"]},
                {"required": ["defaultStatus"]}
            ]
        }
    ],
    "properties": {
        "vendor": {
            "type": "string",
```

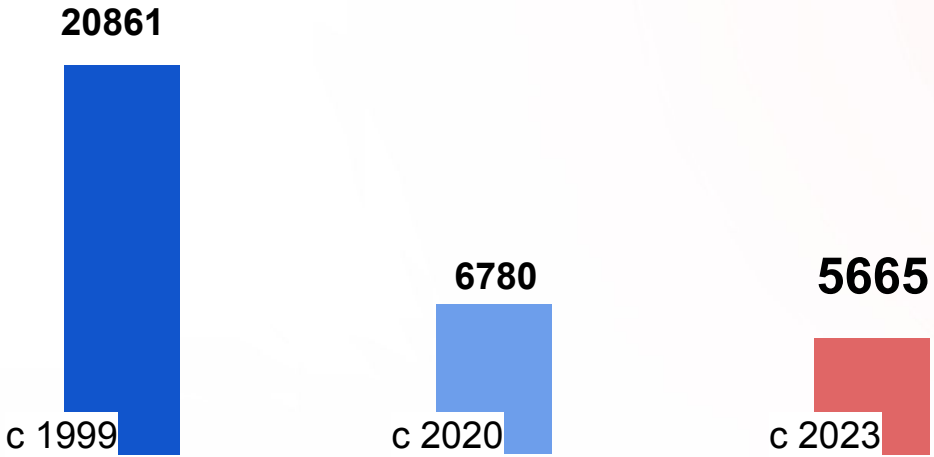
- "unknown"
- "unaffected"
- "affected"

https://github.com/CVEProject/cve-schema/blob/main/schema/CVE_Record_Format.json#L105

1. Если вы дошли до конца - и нигде не было “да”, то у вас точно НЕ фолз

2. А если фолз - не забудьте отправить репорт в тулинг, чтобы это поправили.

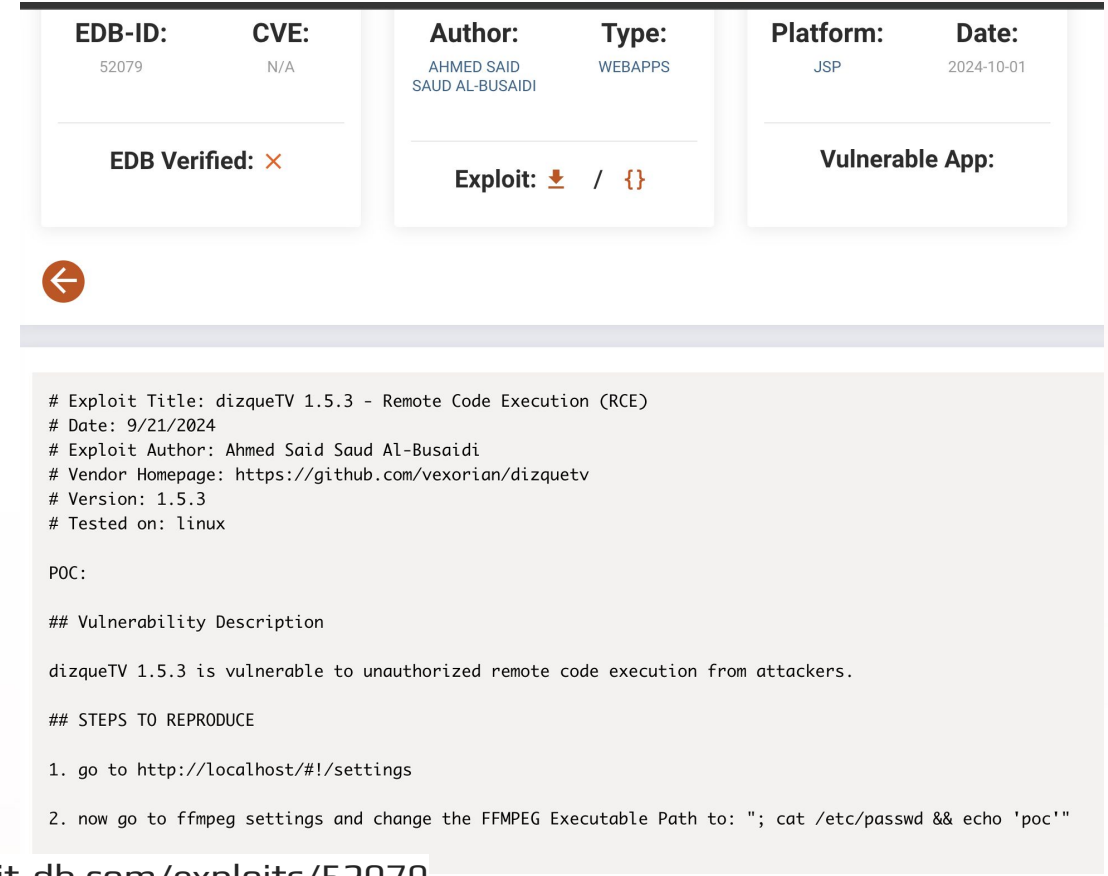
# Слайд для мотивации




CVE.org

количество **уязвимостей с известными эксплойтами** на ноябрь 2024-го

# Exploit DB Sample without




https://www.exploit-db.com/exploits/52079

# **Если хочется добавки** (если вы еще не устали от всех этих сокращений)

1. Non-Actionable Findings in 3rd-party Security Scanners...and How to Identify Them (свежая, о том же о чем последняя часть доклада)

2. Походить самостоятельно по всем ссылкам из презентации. А слайды можно забрать тут: https://github.com/xnuinside/conf_slides и на сайте https://devoops.ru/

3. Посмотреть тулинг с слайда 6

# Не забудьте накидать помидоров в отзывы

*ссылка на github*

https://github.com/xnuinside