Архивы уязвимостей

И как их готовить 

Андрей Кулешов

LOMONOSOV MOSCOW STATE UNIVERSITY

intel

Deutsche Bank

HUAWEI

COSV

https://github.com/akuleshov7

saveourtool/save-cloud Public

Cluster-based cloud mechanism for running SAVE framework

Kotlin 38 3

saveourtool/diktat Public

Strict coding standard for Kotlin and a custom set of rules for detecting code smells, code style issues and bugs

Kotlin 494 37

В предыдущих сериях

ДОКЛАД Security XML 13.10 / 16:15 – 17:00 (UTC+3)

Как обработка XML приводит к проблемам с безопасностью? Разбираемся с XXE

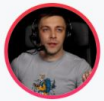
RU

Презентация pdf

Обработка XML может приводить к неожиданным проблемам с безопасностью приложений. Например, к утечкам данных. Как? Этому и будет посвящён доклад.

Основная тема — уязвимость XXE. Поговорим о том, из-за чего вообще при работе с XML возникают дефекты безопасности. Разберёмся с тем, какие виды XXE бывают и в чём их особенности. Конечно, затронем вопросы атаки и защиты. Для лучшего понимания материала спикер продемонстрирует примеры реальных уязвимостей из open source-проектов.

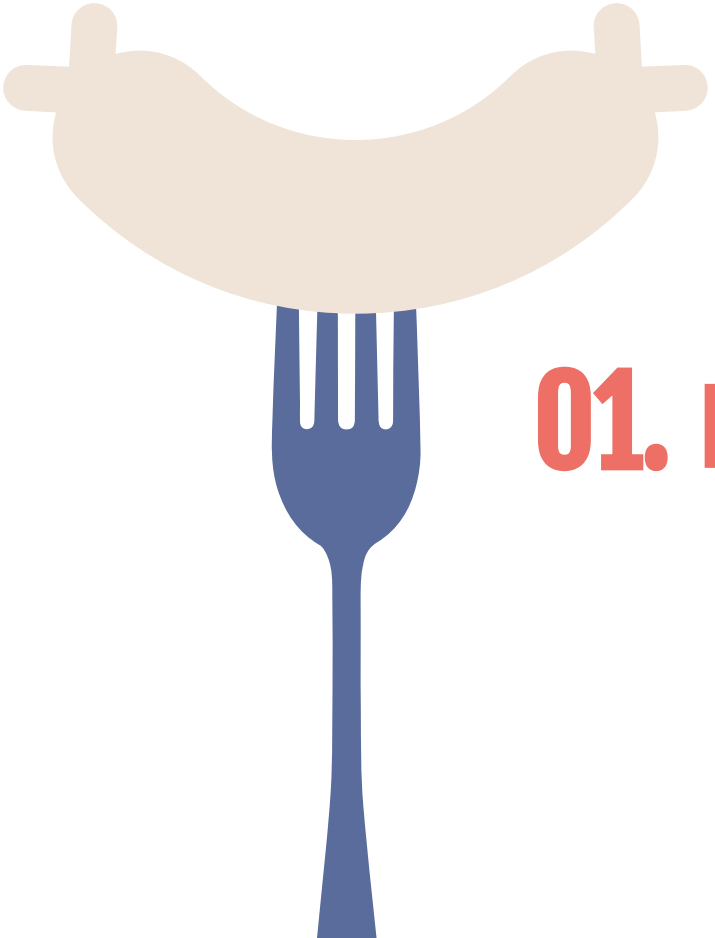
Спикеры



Сергей Васильев

Приглашенные эксперты

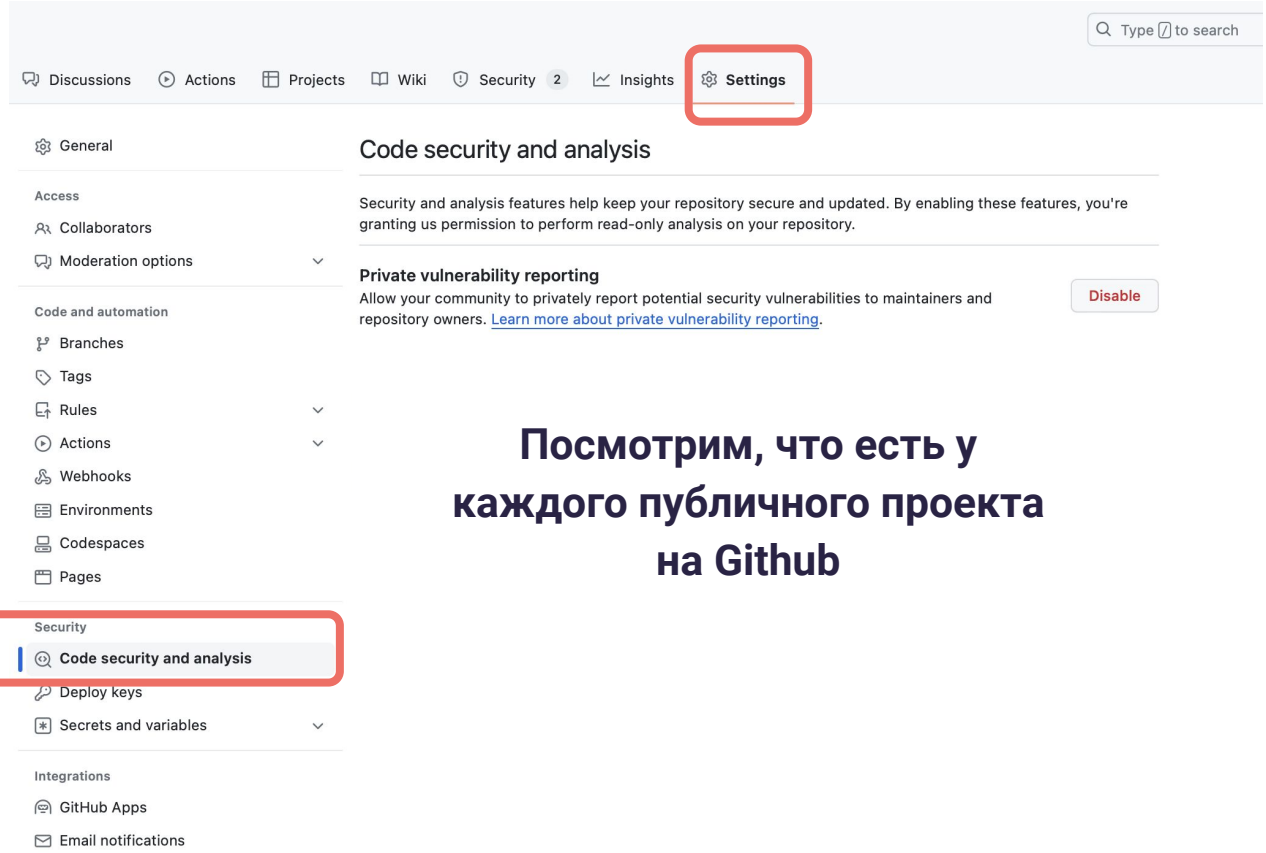
Андрей Когунь
КРОК



01. Проблематика

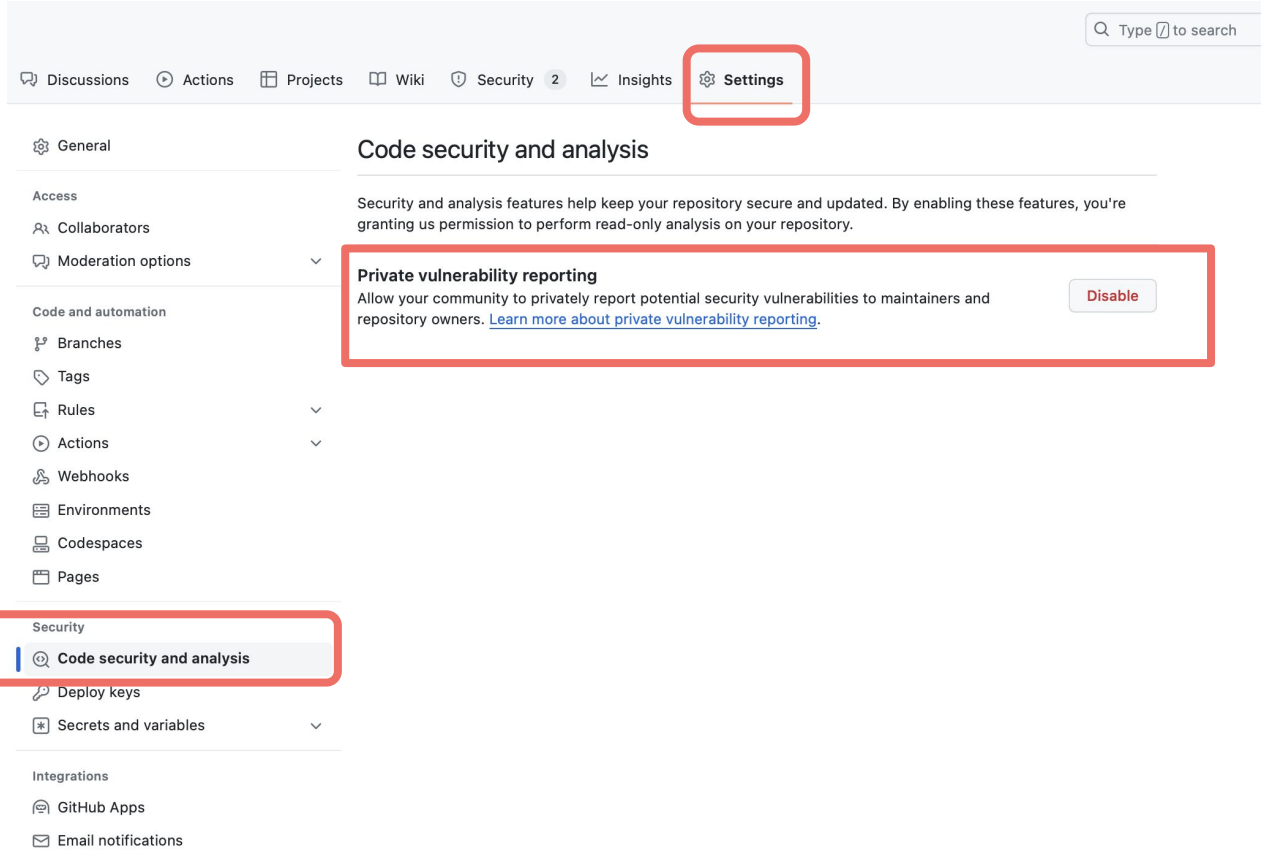
Разбираемся на котиках – на примере GH

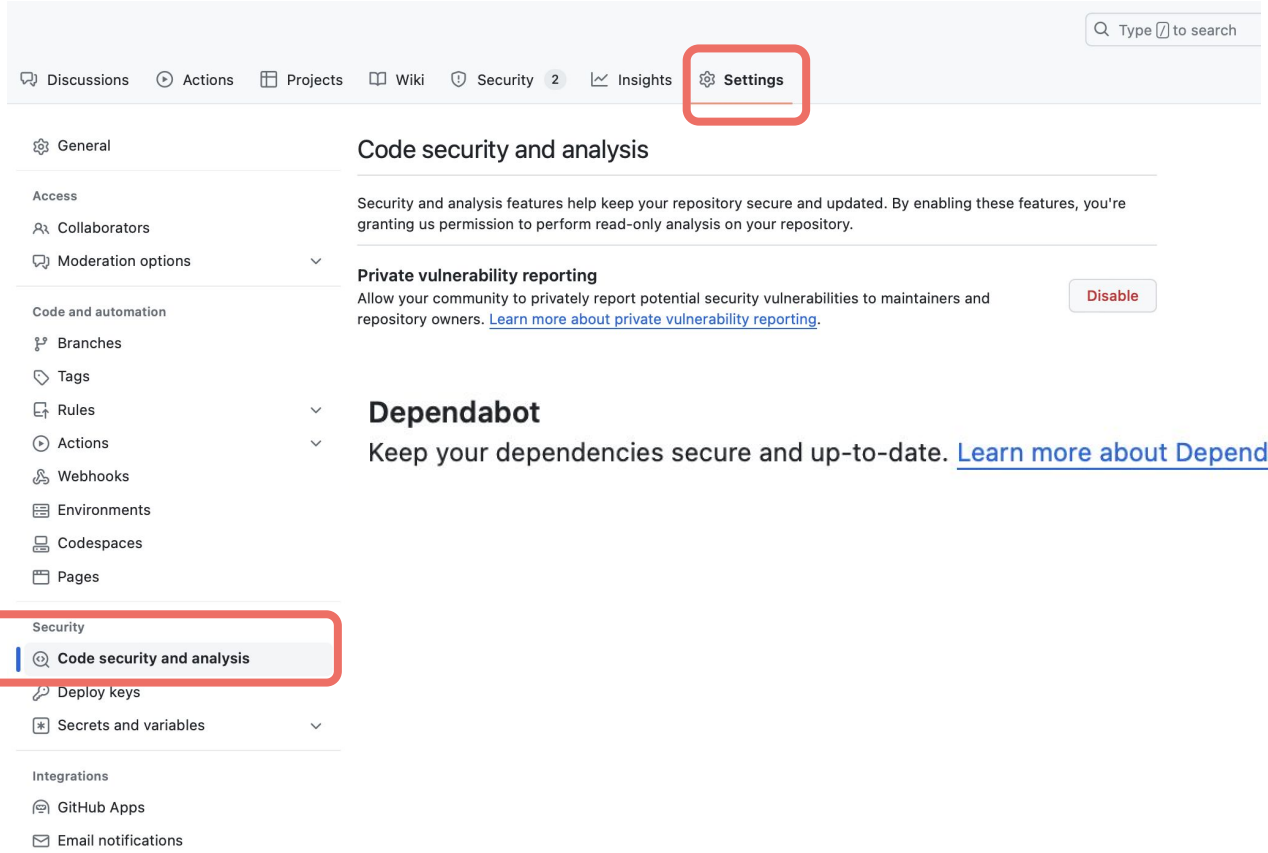
Github Security R&D lab

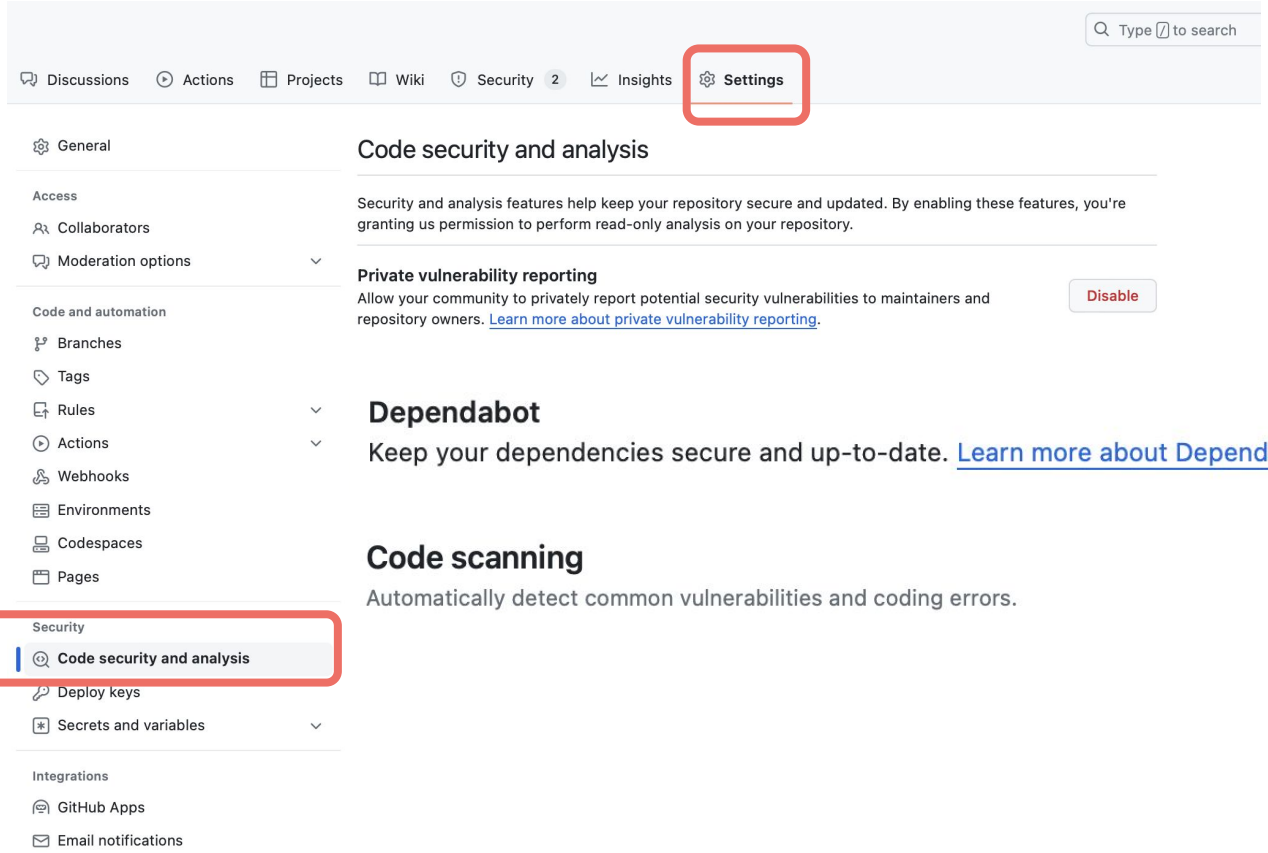


Посмотрим, что есть у каждого публичного проекта на Github

https://github.com/user/project/settings/security_analysis

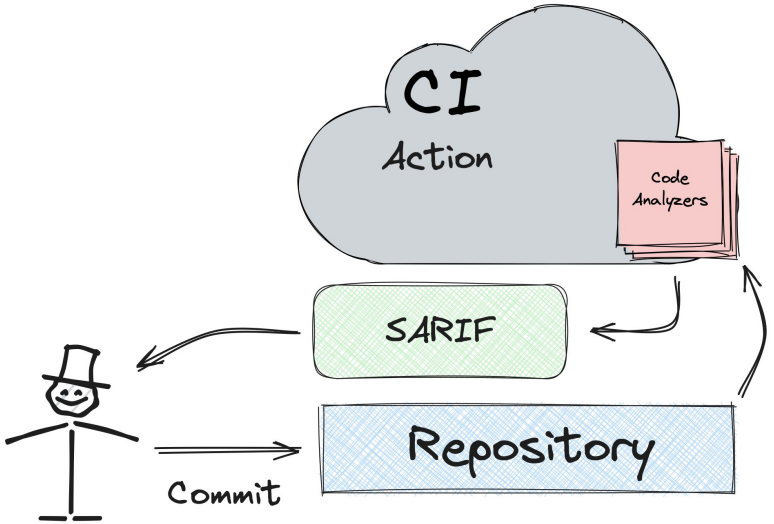

Type / to search
Discussions
Actions
Projects
Wiki
Security 2
Insights
Settings
General
Access
Collaborators
Moderation options
Code and automation
Branches
Tags
Rules
Actions
Webhooks
Environments
Codespaces
Pages
Security
Code security and analysis
Deploy keys
Secrets and variables
Integrations
GitHub Apps
Email notifications
Code security and analysis
Security and analysis features help keep your repository secure and updated. By enabling these features, you're granting us permission to perform read-only analysis on your repository.
Private vulnerability reporting
Allow your community to privately report potential security vulnerabilities to maintainers and repository owners. Learn more about private vulnerability reporting.
Disable


Type / to search
Discussions
Actions
Projects
Wiki
Security 2
Insights
Settings
General
Access
Collaborators
Moderation options
Code and automation
Branches
Tags
Rules
Actions
Webhooks
Environments
Codespaces
Pages
Security
Code security and analysis
Deploy keys
Secrets and variables
Integrations
GitHub Apps
Email notifications
Code security and analysis
Security and analysis features help keep your repository secure and updated. By enabling these features, you're granting us permission to perform read-only analysis on your repository.
Private vulnerability reporting
Allow your community to privately report potential security vulnerabilities to maintainers and repository owners. Learn more about private vulnerability reporting.
Disable
Dependabot
Keep your dependencies secure and up-to-date. Learn more about Dependabot.


Type / to search
Discussions
Actions
Projects
Wiki
Security 2
Insights
Settings
General
Access
Collaborators
Moderation options
Code and automation
Branches
Tags
Rules
Actions
Webhooks
Environments
Codespaces
Pages
Security
Code security and analysis
Deploy keys
Secrets and variables
Integrations
GitHub Apps
Email notifications
Code security and analysis
Security and analysis features help keep your repository secure and updated. By enabling these features, you're granting us permission to perform read-only analysis on your repository.
Private vulnerability reporting
Allow your community to privately report potential security vulnerabilities to maintainers and repository owners. Learn more about private vulnerability reporting.
Disable
Dependabot
Keep your dependencies secure and up-to-date. Learn more about Dependabot.
Code scanning
Automatically detect common vulnerabilities and coding errors.

Source Code Scan

Сканирование изменений



Source Code Scan

Сканирование изменений

save-frontend/build.gradle.kts Fixed — Hide fixed

```
277 +     tasks.forEach {
278 +         println(it.name)
279 +     }
280 + }
```

Check failure

Code scanning / ktlint

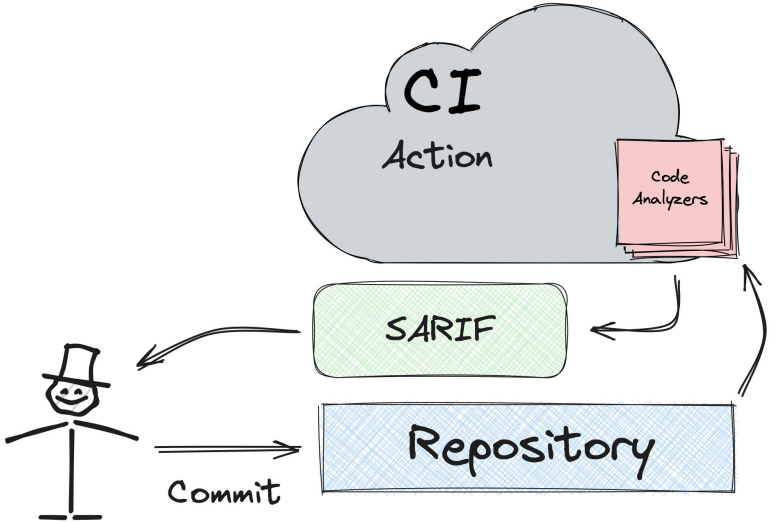
[WRONG_INDENTATION] only spaces are allowed for indentation and each indentation should equal to 4 spaces (tabs are not allowed): no newline at the end of file build.gradle.kts — Error

[WRONG_INDENTATION] only spaces are allowed for indentation and each indentation should equal to 4 spaces (tabs are not allowed): no newline at the end of file build.gradle.kts

Show more details

Dismiss alert

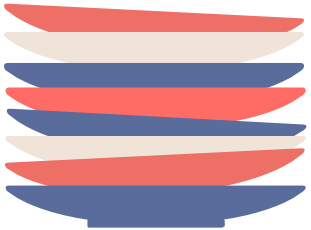
Reply...



SARIF

OASIS OPEN

Static **A**nalysis **R**esults
Interchange **F**ormat



```
{
  "version": "2.1.0",
  "$schema": "http://json.schemastore.org/sarif-2.1.0-rtm.4",
  "runs": [
    {
         ...

    "results": [
        {
          "level": "error",
          "message": {
            "text": "'x' is assigned a value but never used."
          },
          "locations": [
            {
              "physicalLocation": {
                "artifactLocation": {
                  "uri": "file:///C:/dev/example.js",
                  "index": 0
                },
                "region": {
                  "startLine": 1,
                  "startColumn": 5
                }
              }
            }
          ],
          "ruleId": "no-unused-vars",
          "ruleIndex": 0
        }
      ]
    }
  ]
}
```

Загрузка SARIF'ов

`upload-sarif`

Github предоставляет стандартный API для загрузки репортов

Загрузка SARIF'ов

`upload-sarif`

Github предоставляет стандартный API для загрузки репортов

```
- name: Upload SARIF report to Github
  uses: github/codeql-action/upload-sarif@v3
  if: ${{ failure() }}
  with:
    sarif_file: build/diktat-sarif-reports
```

Source Code Scan: CodeQl

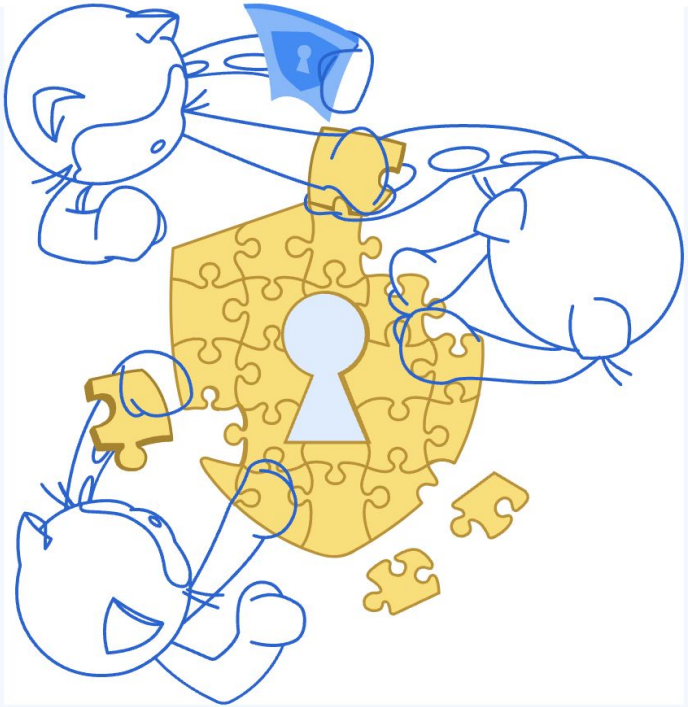
https://docs.github.com/en/code-security/code-scanning

```
/**
* @id java/examples/tryfinally
* @name Try-finally statements
* @description Finds try-finally statements without a catch clause
* @tags try
*       finally
*       catch
*       exceptions
*/

import java

from TryStmt t
where
exists(t.getFinally()) and
not exists(t.getACatchClause())
select t
```

Source Code Scan: CodeQl



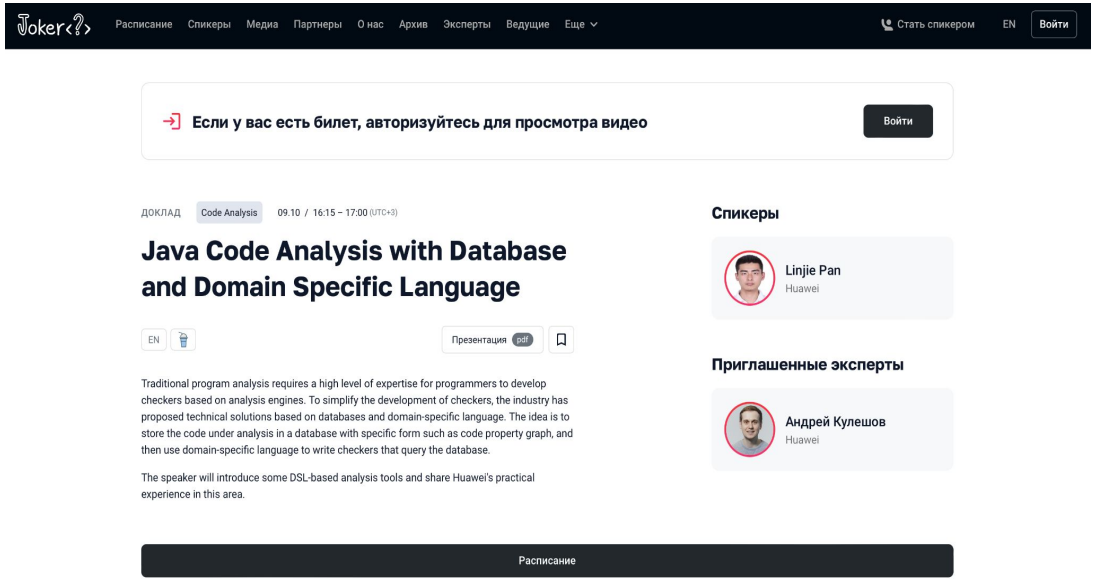
NEW: Special program for Swift and Kotlin!

With CodeQL support for Swift and Kotlin now in public Beta, GitHub Security Lab is including temporarily these languages as part of the supported languages for its CodeQL Bug Bounty program. During 6 months, up to December 1, 2023, Swift and Kotlin submissions will be accepted, and the best ones will be awarded special bonuses.

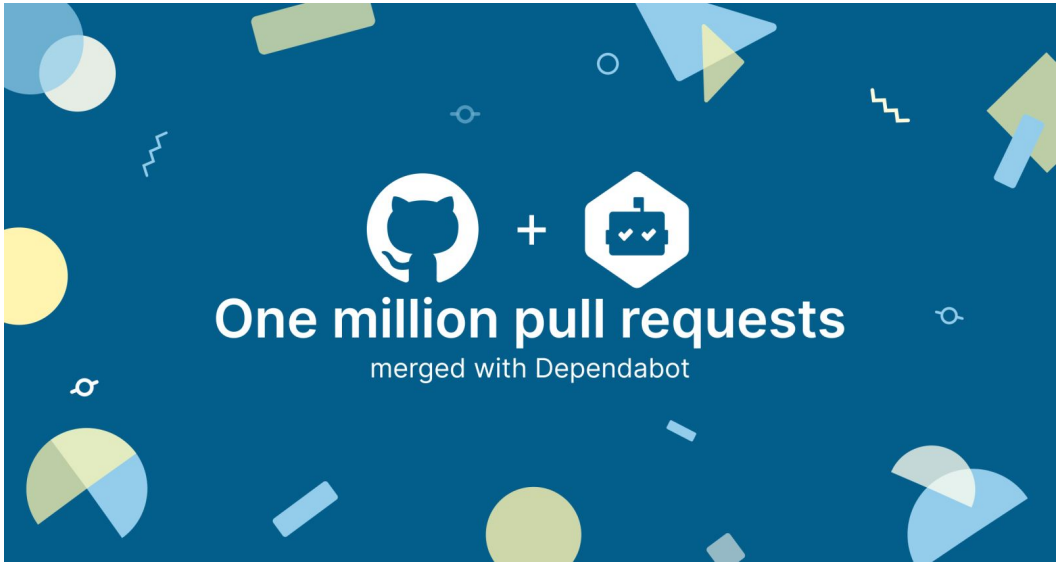
The first 10 submissions that score High or Critical could get an additional reward of **up to $2,000!**

This special bonus program will run for a limited time, for submissions before **December 1, 2023.**

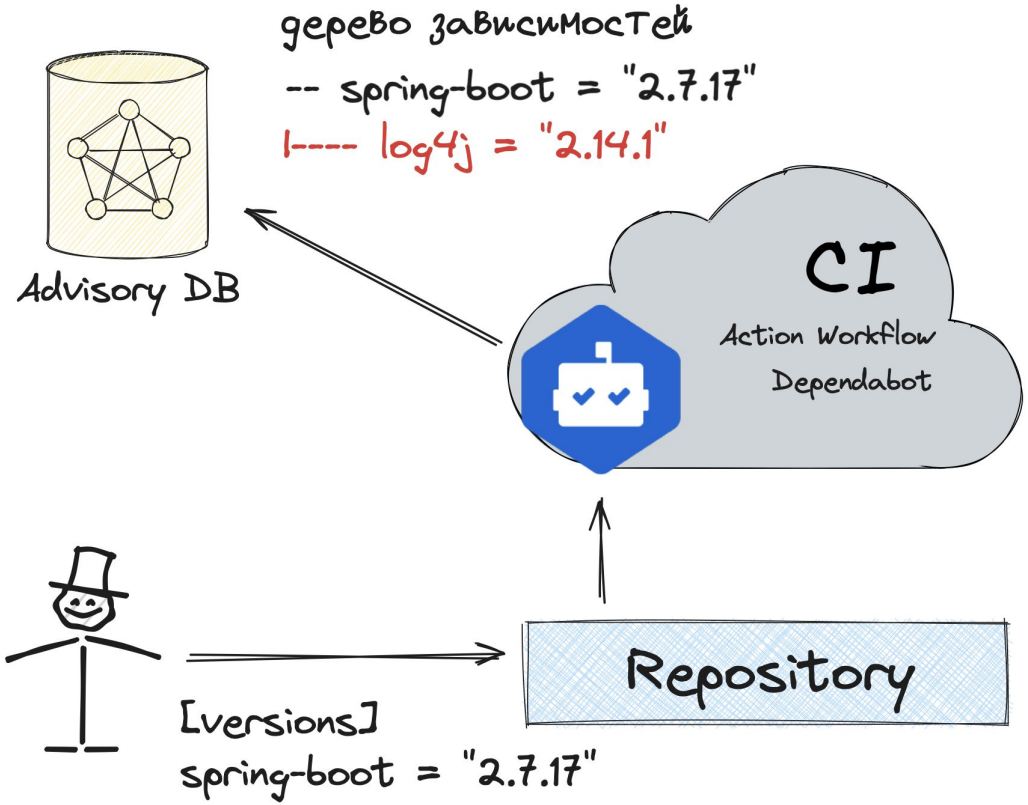
Source Code Scan: CodeQl



Dependency Scan

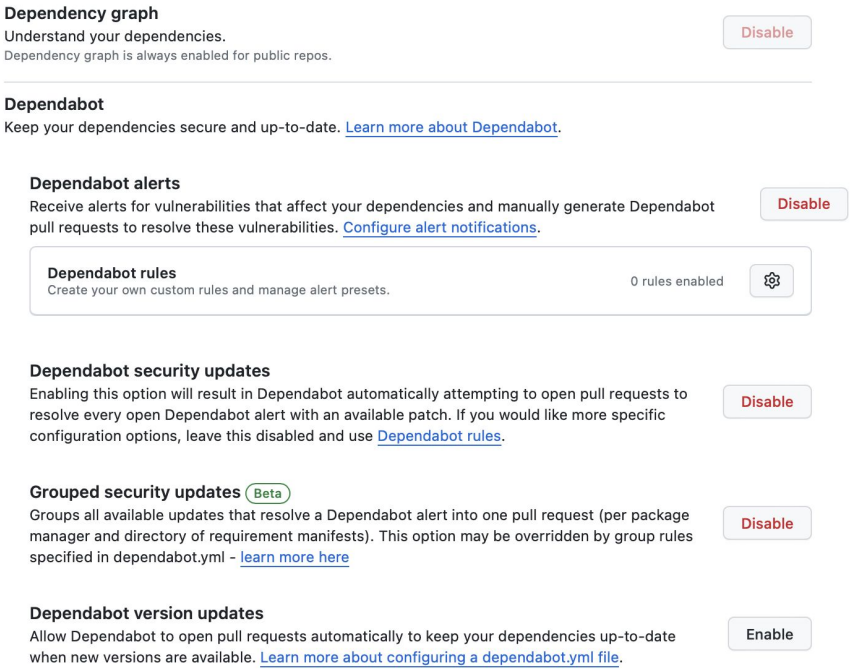


July 25, 2019


дерево зависимостей
-- spring-boot = "2.7.17"
|---- log4j = "2.14.1"
Advisory DB
CI
Action Workflow
Dependabot
Repository
[versions]
spring-boot = "2.7.17"

Dependabot Scan

- Граф зависимостей, но **есть нюанс**
- Авто-обновление зависимостей через PR
- Нотификации об уязвимостях



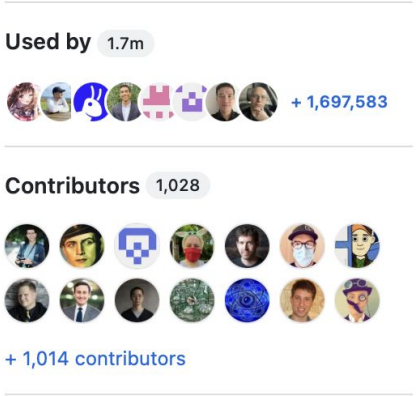
Нюанс

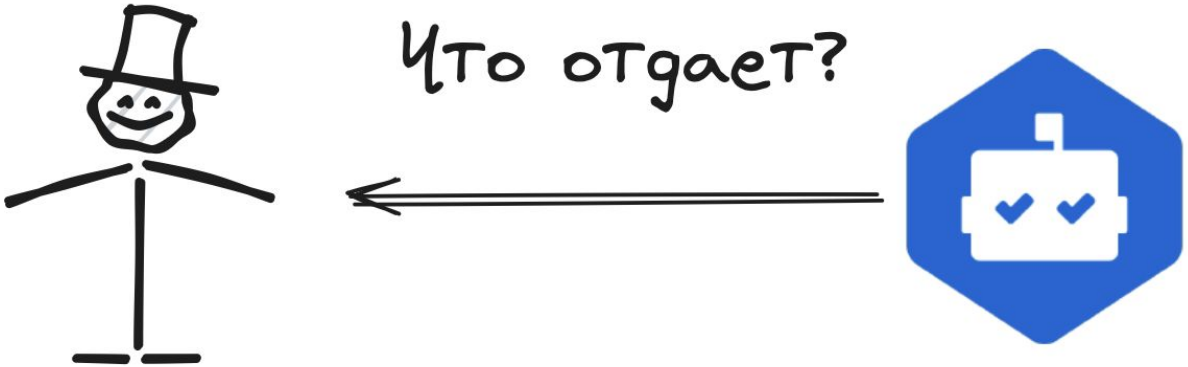
Cargo	Rust
Composer	PHP
NuGet	.NET languages (C#, F#, VB), C++
GitHub Actions	YAML
Go modules	Go
Maven	Java, Scala
npm	JavaScript
pip	Python
pnpm	JavaScript
pub	Dart
Python Poetry	Python
RubyGems	Ruby
Swift Package Manager	Swift
Yarn	JavaScript

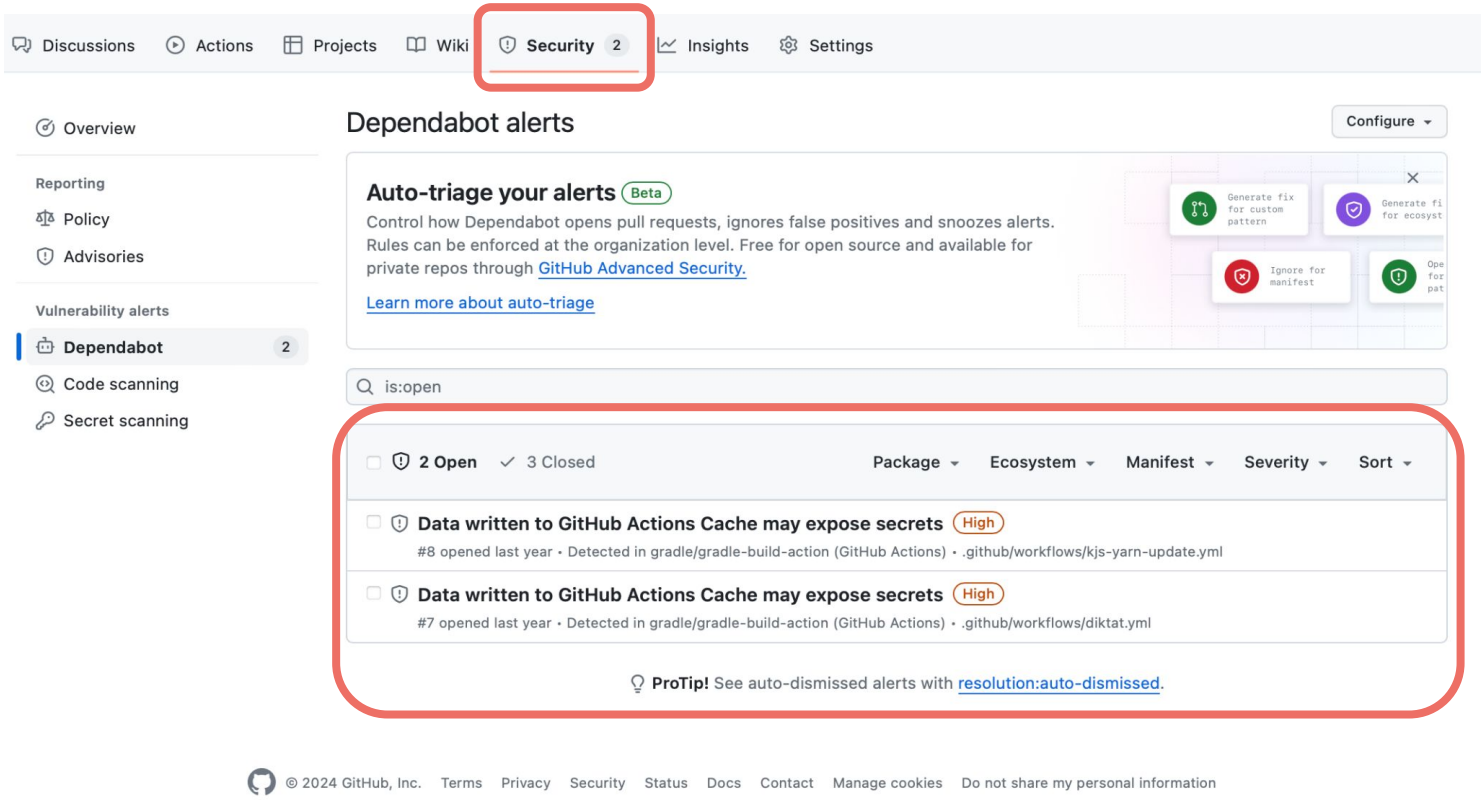
Gradle?

SBT?

Kotlin?




Что отдает?


Discussions
Actions
Projects
Wiki
Security 2
Insights
Settings
Overview
Reporting
Policy
Advisories
Vulnerability alerts
Dependabot 2
Code scanning
Secret scanning
Dependabot alerts
Configure
Auto-triage your alerts Beta
Control how Dependabot opens pull requests, ignores false positives and snoozes alerts. Rules can be enforced at the organization level. Free for open source and available for private repos through GitHub Advanced Security.
Learn more about auto-triage
is:open
2 Open
3 Closed
Package
Ecosystem
Manifest
Severity
Sort
Data written to GitHub Actions Cache may expose secrets High
#8 opened last year • Detected in gradle/gradle-build-action (GitHub Actions) • .github/workflows/kjs-yarn-update.yml
Data written to GitHub Actions Cache may expose secrets High
#7 opened last year • Detected in gradle/gradle-build-action (GitHub Actions) • .github/workflows/diktat.yml
ProTip! See auto-dismissed alerts with resolution:auto-dismissed.
© 2024 GitHub, Inc.
Terms
Privacy
Security
Status
Docs
Contact
Manage cookies
Do not share my personal information

Dependabot alerts / #8

Data written to GitHub Actions Cache may expose secrets #8

Dismiss alert

Open · Opened last year on **gradle/gradle-build-action** (GitHub Actions) · .github/workflows/kjs-yarn-update.yml

⚠ **No security update is needed as gradle/gradle-build-action is no longer vulnerable**

Dependabot hasn't attempted to update gradle/gradle-build-action as it's no longer vulnerable.

Try again | Learn more about troubleshooting Dependabot errors

Package	Affected versions	Patched version
gradle/gradle-build-action (GitHub Actions)	`< 2.4.2`	`2.4.2`

Impact

This vulnerability impacts GitHub workflows using the Gradle Build Action that have executed the Gradle Build Tool with the configuration cache enabled, potentially exposing secrets configured for the repository.

Secrets configured for GitHub Actions are normally passed to the Gradle Build Tool via environment variables. Due to the way that the Gradle Build Tool records these environment variables, they may be persisted into an entry in the GitHub Actions cache. This data stored in the GitHub Actions cache can be read by a GitHub Actions workflow running in an untrusted context, such as that running for a Pull Request submitted by a developer via a repository fork.

This vulnerability was discovered internally through code review, and we have not seen any evidence of it being exploited in the wild. However, in addition to upgrading the Gradle Build Action, you should delete any potentially vulnerable cache entries and may choose to rotate any potentially affected secrets (see Remediation).

Patches

Gradle Build Action v2.4.2 (and newer) no longer save this sensitive data for later use, preventing ongoing leakage of secrets via the GitHub Actions Cache. We strongly recommend that all users of the Gradle Build Action upgrade to `v2.4.2` (or simply `v2`) immediately.

Remediation

While upgrading to the latest version of the Gradle Build Action will prevent leakage of secrets going forward, additional actions may be required due to current or previous GitHub Actions Cache entries containing this information.

Severity

High 7.6 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	Required
Scope	Changed
Confidentiality	High
Integrity	Low
Availability	None

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

Tags

Runtime dependency | Patch available

Weaknesses

CWE-200

CWE-312

CVE ID

CVE-2023-30853

GHSA ID

GHSA-h3qr-39j9-4r5v

See advisory in GitHub Advisory Database

See all of your affected repositories

See something to contribute?
Suggest improvements for this advisory on the GitHub Advisory Database.

Dependabot alerts / #8

Data written to GitHub Actions Cache may expose secrets #8

Dismiss alert

Open — Opened last year on **gradle/gradle-build-action** (GitHub Actions) · .github/workflows/kjs-yarn-update.yml

No security update is needed as gradle/gradle-build-action is no longer vulnerable

Dependabot hasn't attempted to update gradle/gradle-build-action as it's no longer vulnerable.

Try again | Learn more about troubleshooting Dependabot errors

Package	Affected versions	Patched version
gradle/gradle-build-action (GitHub Actions)	< 2.4.2	2.4.2

Impact

This vulnerability impacts GitHub workflows using the Gradle Build Action that have executed the Gradle Build Tool with the configuration cache enabled, potentially exposing secrets configured for the repository.

Secrets configured for GitHub Actions are normally passed to the Gradle Build Tool via environment variables. Due to the way that the Gradle Build Tool records these environment variables, they may be persisted into an entry in the GitHub Actions cache. This data stored in the GitHub Actions cache can be read by a GitHub Actions workflow running in an untrusted context, such as that running for a Pull Request submitted by a developer via a repository fork.

This vulnerability was discovered internally through code review, and we have not seen any evidence of it being exploited in the wild. However, in addition to upgrading the Gradle Build Action, you should delete any potentially vulnerable cache entries and may choose to rotate any potentially affected secrets (see Remediation).

Patches

Gradle Build Action v2.4.2 (and newer) no longer save this sensitive data for later use, preventing ongoing leakage of secrets via the GitHub Actions Cache. We strongly recommend that all users of the Gradle Build Action upgrade to `v2.4.2` (or simply `v2`) immediately.

Remediation

While upgrading to the latest version of the Gradle Build Action will prevent leakage of secrets going forward, additional actions may be required due to current or previous GitHub Actions Cache entries containing this information.

Severity

High 7.6 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	Required
Scope	Changed
Confidentiality	High
Integrity	Low
Availability	None

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

Tags

Runtime dependency | Patch available

Weaknesses

CWE-200

CWE-312

CVE ID

CVE-2023-30853

GHSA ID

GHSA-h3qr-39j9-4r5v

See advisory in GitHub Advisory Database

See all of your affected repositories

See something to contribute?
Suggest improvements for this advisory on the GitHub Advisory Database.

Dependabot alerts / #8

Data written to GitHub Actions Cache may expose secrets #8

Dismiss alert

Open — Opened last year on **gradle/gradle-build-action** (GitHub Actions) · .github/workflows/kjs-yarn-update.yml

⚠ **No security update is needed as gradle/gradle-build-action is no longer vulnerable**

Dependabot hasn't attempted to update gradle/gradle-build-action as it's no longer vulnerable.

Try again | Learn more about troubleshooting Dependabot errors

Package	Affected versions	Patched version
gradle/gradle-build-action (GitHub Actions)	< 2.4.2	2.4.2

Impact

This vulnerability impacts GitHub workflows using the Gradle Build Action that have executed the Gradle Build Tool with the configuration cache enabled, potentially exposing secrets configured for the repository.

Secrets configured for GitHub Actions are normally passed to the Gradle Build Tool via environment variables. Due to the way that the Gradle Build Tool records these environment variables, they may be persisted into an entry in the GitHub Actions cache. This data stored in the GitHub Actions cache can be read by a GitHub Actions workflow running in an untrusted context, such as that running for a Pull Request submitted by a developer via a repository fork.

This vulnerability was discovered internally through code review, and we have not seen any evidence of it being exploited in the wild. However, in addition to upgrading the Gradle Build Action, you should delete any potentially vulnerable cache entries and may choose to rotate any potentially affected secrets (see Remediation).

Patches

Gradle Build Action v2.4.2 (and newer) no longer save this sensitive data for later use, preventing ongoing leakage of secrets via the GitHub Actions Cache. We strongly recommend that all users of the Gradle Build Action upgrade to `v2.4.2` (or simply `v2`) immediately.

Remediation

While upgrading to the latest version of the Gradle Build Action will prevent leakage of secrets going forward, additional actions may be required due to current or previous GitHub Actions Cache entries containing this information.

Severity

High 7.6 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	Required
Scope	Changed
Confidentiality	High
Integrity	Low
Availability	None

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

Tags

Runtime dependency | Patch available

Weaknesses

CWE-200

CWE-312

CVE ID

CVE-2023-30853

GHSA ID

GHSA-h3qr-39j9-4r5v

See advisory in GitHub Advisory Database

See all of your affected repositories

See something to contribute?
Suggest improvements for this advisory on the GitHub Advisory Database.

Bump the github_actions group across 1 directory with 1 update #262

Edit | Code

Open **dependabot** wants to merge 1 commit into `main` from `dependabot/github_actions/dot-github/workflows/github_actions-security-group-4a94bdf9ab`

Conversation 0 | Commits 1 | Checks 3 | Files changed 2 | +2 −2

dependabot bot commented on behalf of **github** 1 minute ago

Bumps the github_actions group with 1 update in the /.github/workflows directory: gradle/gradle-build-action.

Updates `gradle/gradle-build-action` from 2 to 3

▶ Release notes

▶ Commits

compatibility unknown

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

▶ Dependabot commands and options

Bump the github_actions group across 1 directory with 1 update ··· Verified 5999a42

dependabot bot added dependencies github_actions labels 1 minute ago

Add more commits by pushing to the **dependabot/github_actions/dot-github/workflows/github_actions-security-group-4a94bdf9ab** branch on **akuleshov7/ktoml**.

This branch has not been deployed
No deployments

Reviewers
Suggestions
akuleshov7 Request
At least 1 approving review is required to merge this pull request.
Still in progress? Convert to draft

Assignees
No one—assign yourself

Labels
dependencies github_actions

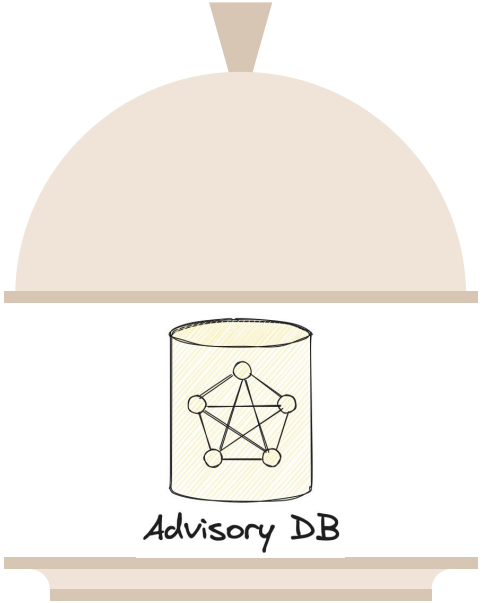
Projects
None yet

Milestone
No milestone

Development
Successfully merging this pull request may close these issues.
None yet

Notifications Customize
Unsubscribe

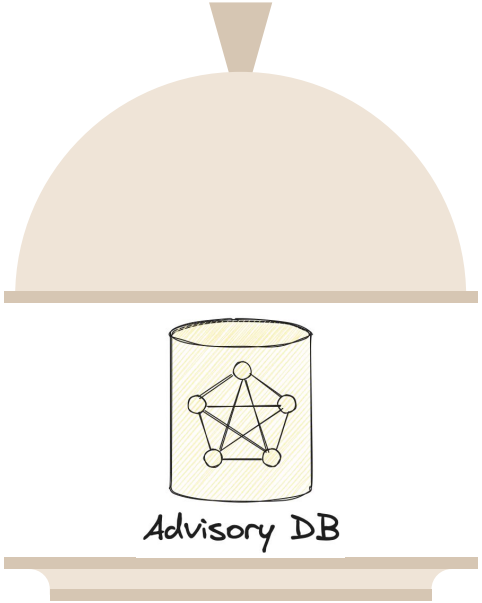
Базы/архивы Уязвимостей



Основное блюдо

- Базы данных, агрегирующие массу **one-day** уязвимостей
- Изредка позволяя репортить **приватные** уязвимости

Базы/архивы Уязвимостей



Основное блюдо

- Базы данных, агрегирующие массу **one-day** уязвимостей
- Изредка позволяя репортить **приватные** уязвимости

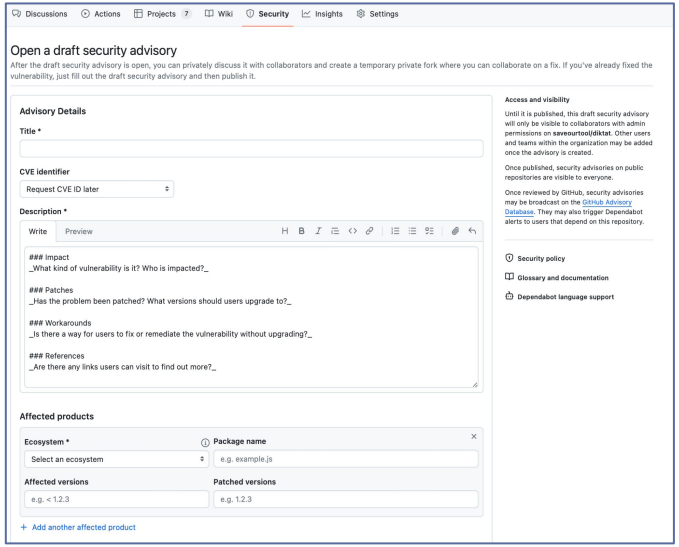
Функционал

- Поиск, фильтрация, подключение API
- Репортинг, ревью, агрегация

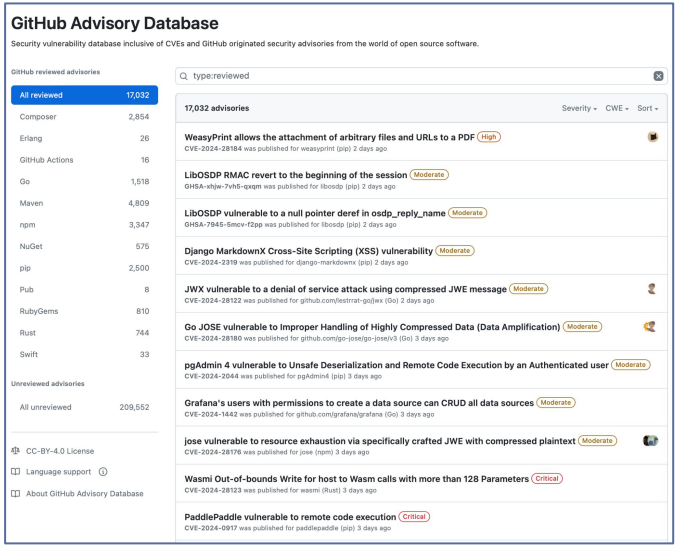
02.

Обзор того, что уже есть

ZERO-DAY



ONE-DAY



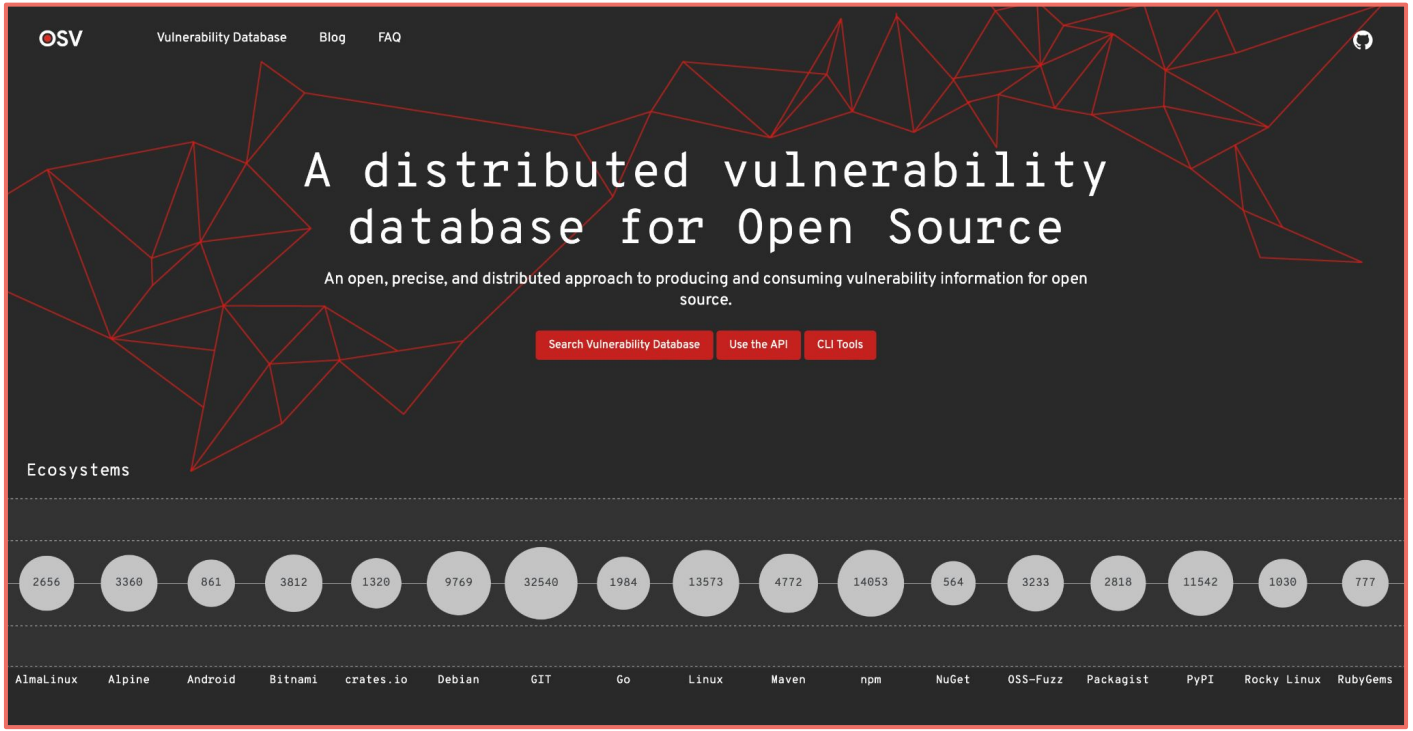
200,000+

All unreviewed

17,000+

Reviewed

И потребовалась нормализация



https://osv.dev/

OSV.dev

google / osv.dev

Платформа и API

Распределенная платформа для сбора и хранения существующих

Схема

Участие в проекте схемы OSV

Авторы последней версии:

- Oliver Chang (ochang@**google**.com)
- Russ Cox (rsc@**google**.com)

Клиенты и сканер

OSV-scanner

OSV.dev

google / osv.dev

Платформа и API

Распределенная платформа для сбора и хранения существующих

Схема!

Участие в проекте схемы OSV

Авторы последней версии:

- Oliver Chang (ochang@**google**.com)
- Russ Cox (rsc@**google**.com)

Клиенты и сканер

OSV-scanner

Open Source Vulnerability Schema

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

- JSON схема, последней версии 1.6.2
- `{ "id": string, "modified": string }`

`<DB>`—`<ENTRYID>, Время последнего обновления`

Rocky Linux Security Advisory Database

Rocky Linux Security Advisory Database

Haskell Security Advisory Database

Python Software Foundation Vulnerability Database

Android Vulnerability Database

AlmaLinux Security Advisory

RConsortium Advisory Database

Curl CVEs

Bitnami Vulnerability Database

Debian Security Advisory Database
(provided by OSV.dev)

Ubuntu Security Notices

LoopBack Advisory Database

Global Security Database

RustSec Advisory Database

Go Vulnerability Database

VMWare Photon Security Advisory Database

GHSA

GitHub Security Advisory Database

CVE

National Vulnerability Database
(provided by OSV.dev)

GitHub Advisory Database / Unreviewed / CVE-2024-2355

A vulnerability has been found in keerti1924 Secret-Coder...

Low severity | Unreviewed | Published 6 hours ago to the GitHub Advisory Database • Updated 6 hours ago

Package	Affected versions	Patched versions
No package listed— Suggest a package	Unknown	Unknown

Description

A vulnerability has been found in keerti1924 Secret-Coder-PHP-Project 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /secret_coder.sql. The manipulation leads to inclusion of sensitive information in source code. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256315. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

References

- https://nvd.nist.gov/vuln/detail/CVE-2024-2355
- https://github.com/smurf-reigz/security/blob/main/proof-of-concepts/keerti1924%20%5BSecret-Coder-PHP-Project%20Sensitive%20Information%20Disclosure%5D%20on%20secret_coder.sql.md
- https://vuldb.com/?ctiid.256315
- https://vuldb.com/?id.256315

Published by the National Vulnerability Database 6 hours ago

Published to the GitHub Advisory Database 6 hours ago

Last updated 6 hours ago

GHSA

Severity

Low 3.7 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	None
Availability	None

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

Weaknesses

CWE-540

CVE ID

CVE-2024-2355

GHSA ID

GHSA-gmhh-c94r-5hfq

Source code

No known source code

Dependabot alerts are not supported on this advisory because it does not have a package from a supported ecosystem with an affected and fixed version.

Learn more about GitHub language support

See something to contribute? Suggest improvements for this vulnerability.

Conversation 0 | Commits 1 | Checks 2 | Files changed 1 | +18 −2

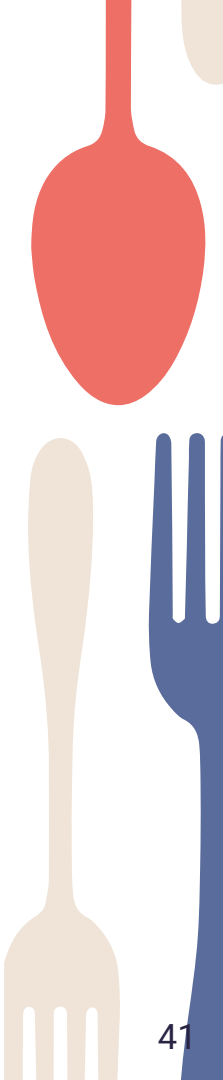
Changes from all commits | File filter | Conversations | Jump to | 0 / 1 files viewed | Review in codespace | Review changes

20 advisories/unreviewed/2024/03/GHSA-gmhh-c94r-5hfq/GHSA-gmhh-c94r-5hfq.json | Viewed

```
@@ -1,11 +1,12 @@
 {
   "schema_version": "1.4.0",
   "id": "GHSA-gmhh-c94r-5hfq",
-  "modified": "2024-03-10T12:30:31Z",
+  "modified": "2024-03-10T12:30:38Z",
   "published": "2024-03-10T12:30:31Z",
   "aliases": [
     "CVE-2024-2355"
   ],
+  "summary": "Unveiling the Risks in keerti1924 Secret-Coder-PHP-Project 1.0",
   "details": "A vulnerability has been found in keerti1924 Secret-Coder-PHP-Project 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /secret_coder.sql. The manipulation leads to inclusion of sensitive information in source code. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256315. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.",
   "severity": [
     {
@@ -14,7 +15,22 @@
     }
   ],
   "affected": [
-
+    {
+      "package": {
+        "ecosystem": "GitHub Actions",
+        "name": ""
+      },
+      "ranges": [
+        {
+          "type": "ECOSYSTEM",
+          "events": [
+            {
+              "introduced": "0"
+            }
+          ]
+        }
+      ]
+    }
   ],
   "references": [
     {
```

OSV database_specific для GHSA

```
"database_specific": {
    "cwe_ids": [
      "CWE-540"
    ],
    "severity": "LOW",
    "github_reviewed": false,
    "github_reviewed_at": null,
    "nvd_published_at": "2024-03-10T12:15:06Z"
  }
```



Third party tools and integrations

There are also community tools that use OSV. Note that these are community built tools and unsupported by the core OSV maintainers.

- Betterscan.io: Code Scanning/SAST/Static Analysis/Linting using many tools/Scanners with One Report (Code, IaC)
- bomber
- Cortex XSOAR
- dependency-management-data
- Dependency-Track
- dep-scan
- EZE-CLI: The one stop shop for security testing in modern development
- G-Rath/osv-detector: A scanner that uses the OSV database.
- GUAC
- it-depends
- .NET client library and support for the schema
- OSS Review Toolkit
- OSV4k: a Java/Kotlin MPP library for serialization and deserialization of OSV schema
- Packj
- pip-audit
- Renovate
- rosv: an R package to access the OSV database and help administer Posit Package Manager
- Rust client library
- Skjold: Security audit python project dependencies against several security advisory databases
- Trivy
- IronDome: SCA scanner for Ruby applications

Наше участие в OSV

https://github.com/saveourtool/osv4k

GitHub Advisory Database / Unreviewed / CVE-2024-2355

A vulnerability has been found in keerti1924 Secret-Coder...

Low severity | Unreviewed | Published 6 hours ago to the GitHub Advisory Database • Updated 6 hours ago

Package	Affected versions	Patched versions
No package listed— Suggest a package	Unknown	Unknown

Description

A vulnerability has been found in keerti1924 Secret-Coder-PHP-Project 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /secret_coder.sql. The manipulation leads to inclusion of sensitive information in source code. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256315. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

References

- https://nvd.nist.gov/vuln/detail/CVE-2024-2355
- https://github.com/smurf-reigz/security/blob/main/proof-of-concepts/keerti1924%20%5BSecret-Coder-PHP-Project%20Sensitive%20Information%20Disclosure%5D%20on%20secret_coder.sql.md
- https://vuldb.com/?ctiid.256315
- https://vuldb.com/?id.256315

Published by the National Vulnerability Database 6 hours ago

Severity

Low 3.7 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	None
Availability	None

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

Weaknesses

CWE-540

CVE ID

CVE-2024-2355

GHSA ID

GHSA-gmhh-c94r-5hfq

Source code

No known source code

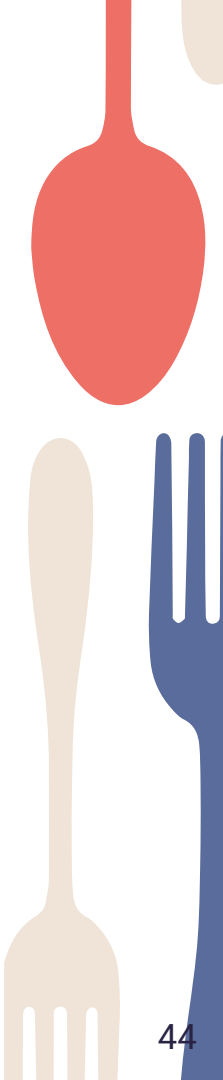
Dependabot alerts are not supported on this advisory because it does not have a package from a supported ecosystem with an affected and fixed version.

Learn more about GitHub language support

See something to contribute? Suggest improvements for this vulnerability.

GHSA

NVD: national vulnerability database



NIST NATIONAL VULNERABILITY DATABASE NVD

NVD: national vulnerability database

*“Vulnerabilities within the NVD are **derived** from the CVE List **which is maintained** by processes upstream of the NVD”*

CVE <–> NVD

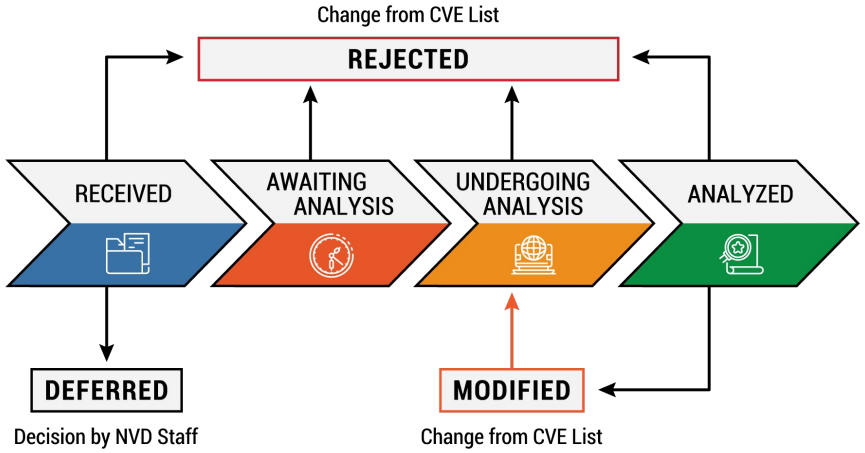
NATIONAL VULNERABILITY DATABASE NVD

NVD: national vulnerability database

*"Vulnerabilities within the NVD are **derived** from the CVE List **which is maintained** by processes upstream of the NVD"*

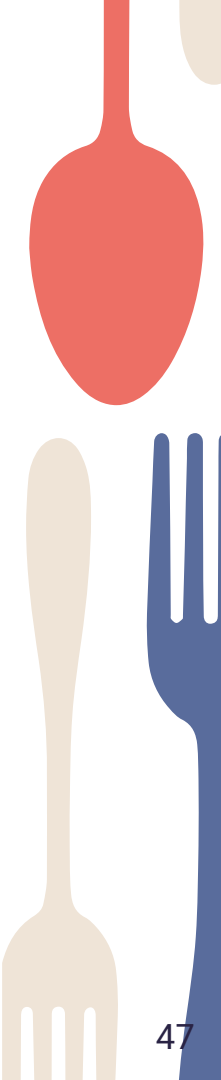
NIST NATIONAL VULNERABILITY DATABASE NVD

CVE <–> NVD



NVD: national vulnerability database

NVD - это база с метаинформацией о CVE



CVE: Common Vulnerabilities and Exposures

CVE: Common Vulnerabilities and Exposures

Request CVE-ID!

Мучились от дубликатов и хотели просто пронумеровать уязвимости

CVE: Common Vulnerabilities and Exposures

Is CVE just another vulnerability database?

"No, CVE is not a vulnerability database. CVE enables the correlation of vulnerability data across tools, databases, and people."

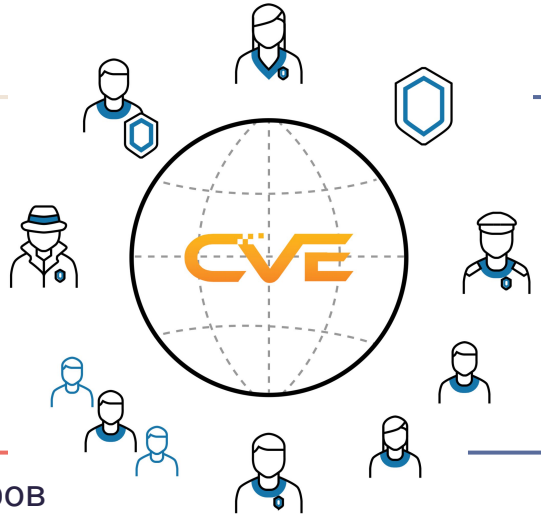
Request CVE-ID!

Мучились от дубликатов и хотели просто пронумеровать уязвимости

CVE: Common Vulnerabilities and Exposures

Is CVE just another vulnerability database?

"No, CVE is not a vulnerability database. CVE enables the correlation of vulnerability data across tools, databases, and people."



Request CVE-ID!

Мучились от дубликатов и хотели просто пронумеровать уязвимости

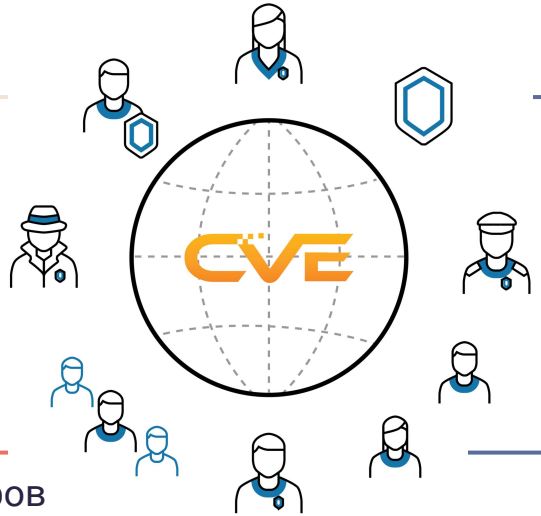
CISA | NIST | MITRE

Участвуют + **365** партнеров

CVE: Common Vulnerabilities and Exposures

Is CVE just another vulnerability database?

"No, CVE is not a vulnerability database. CVE enables the correlation of vulnerability data across tools, databases, and people."



Request CVE-ID!

Мучились от дубликатов и хотели просто пронумеровать уязвимости

CISA | NIST | MITRE

Участвуют + **365** партнеров

Поиск

Только по ID

225к+ уязвимостей

Новости CVE форматов

- CVE JSON Record Format 5.0.0

Новости CVE форматов

- CVE JSON Record Format 5.0.0
- *“Legacy CVE download formats deprecation is now underway and will end on June 30, 2024”*

Новости CVE форматов

- CVE JSON Record Format 5.0.0
- *“Legacy CVE download formats deprecation is now underway and will end on June 30, 2024”*
- *“The OSV team has directly worked with the CVE Quality Working Group on a key new feature of the latest CVE 5.0 standard: a new versioning schema that closely resembles OSV’s own versioning schema. This will enable easy conversion from OSV to CVE 5.0, and vice versa. It also enables OSV to contribute high quality metadata directly back to CVE, and drive better machine readability and data quality across the open source ecosystem.”*

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

CWE: Common Weakness Enumeration

CWE

CWE: Common Weakness Enumeration

CWE: Common Weakness Enumeration

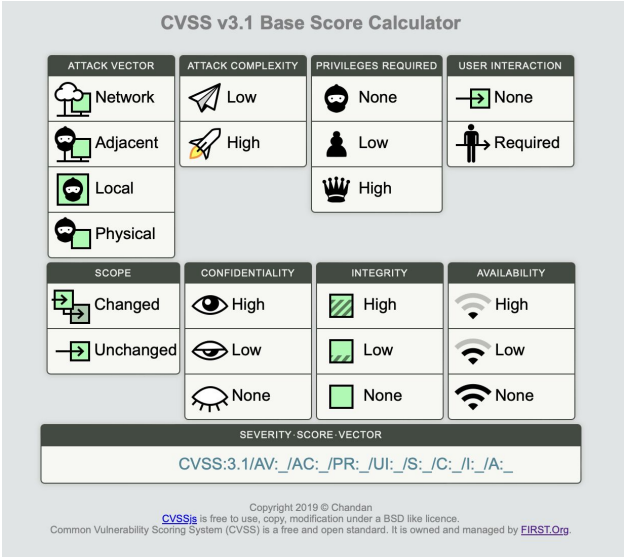
Пример с CWE-502: Deserialization of Untrusted Data

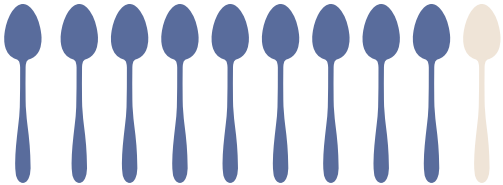
The product deserializes untrusted data without sufficiently verifying that the resulting data will be valid.

Observed Examples

Reference	Description
CVE-2019-12799	chain: bypass of untrusted deserialization issue (CWE-502) by using an assumed-trusted class (CWE-183)
CVE-2015-8103	Deserialization issue in commonly-used Java library allows remote execution.
CVE-2015-4852	Deserialization issue in commonly-used Java library allows remote execution.
CVE-2013-1465	Use of PHP unserialize function on untrusted input allows attacker to modify application configuration.
CVE-2012-3527	Use of PHP unserialize function on untrusted input in content management system might allow code execution.
CVE-2012-0911	Use of PHP unserialize function on untrusted input in content management system allows code execution using a crafted cookie value.
CVE-2012-0911	Content management system written in PHP allows unserialize of arbitrary objects, possibly allowing code execution.
CVE-2011-2520	Python script allows local users to execute code via pickled data.
CVE-2012-4406	Unsafe deserialization using pickle in a Python script.
CVE-2003-0791	Web browser allows execution of native methods via a crafted string to a JavaScript function that deserializes the string.

CVSS - Common Vulnerability Scoring System Version: -> 4.0.0





9/10

HIGH

CPE

OWASP

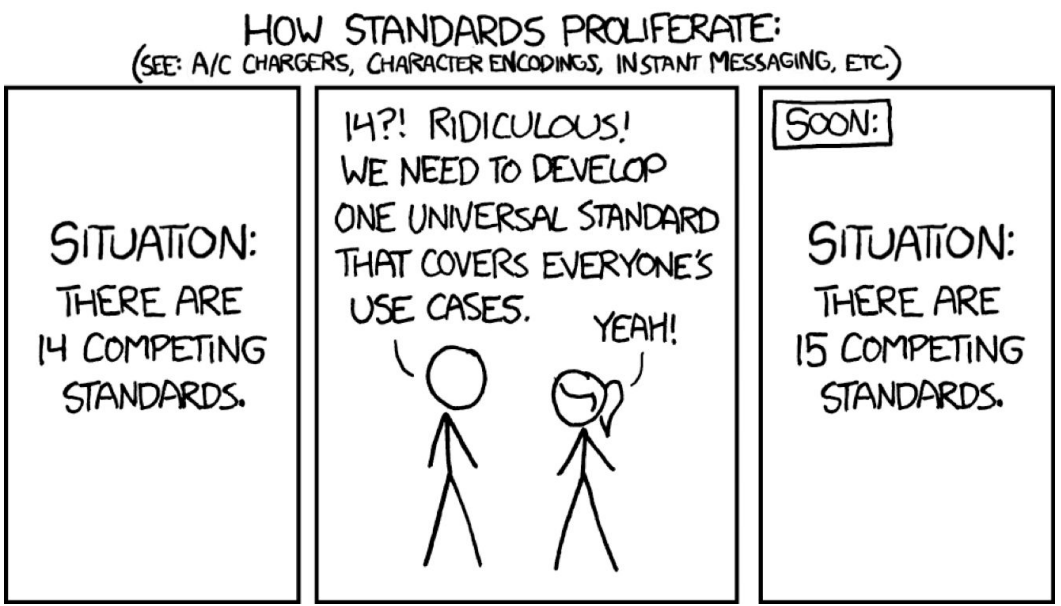
CSAR

CSAF

KEV

03.

China OSV


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

中国计算机学会开源发展委员会（CCF ODC）相关规划
– 构筑中国自主可控的开源漏洞知识图谱服务COSV

	海外				中国					
软件供应链安全SCA产品	Blackduck	Snyk	Mend	...	奇安信开源卫士	棱镜七彩	源图	重睛鸟	CodeArts Governance	...
公开漏洞汇聚服务 系统可直接消费 精准、及时、全面	OSV（开源漏洞汇聚平台） 自动化公开漏洞汇聚 OSV Schema （格式标准）				CCF精准开源漏洞汇聚平台 COSV 自动化公开漏洞汇聚 公开漏洞智能精化 隐匿漏洞补丁提前识别 未知漏洞自动化发现 漏洞数据智能确认平台 COSV Schema 自动化 & 人工					
0-DAY 漏洞上报平台	NVD	CVE	GitHub Security Advisories	PyPI Advisory Database	...	CNVD	CNNVD	CICSVD		
	公共安全漏洞库		领域特定安全情报中心			公共安全漏洞库				

Тайминг по COSV-схеме

Создание OSV-совместимого Формата, удобного для существующих баз

2023/04

Дискуссии среди 8 организаций

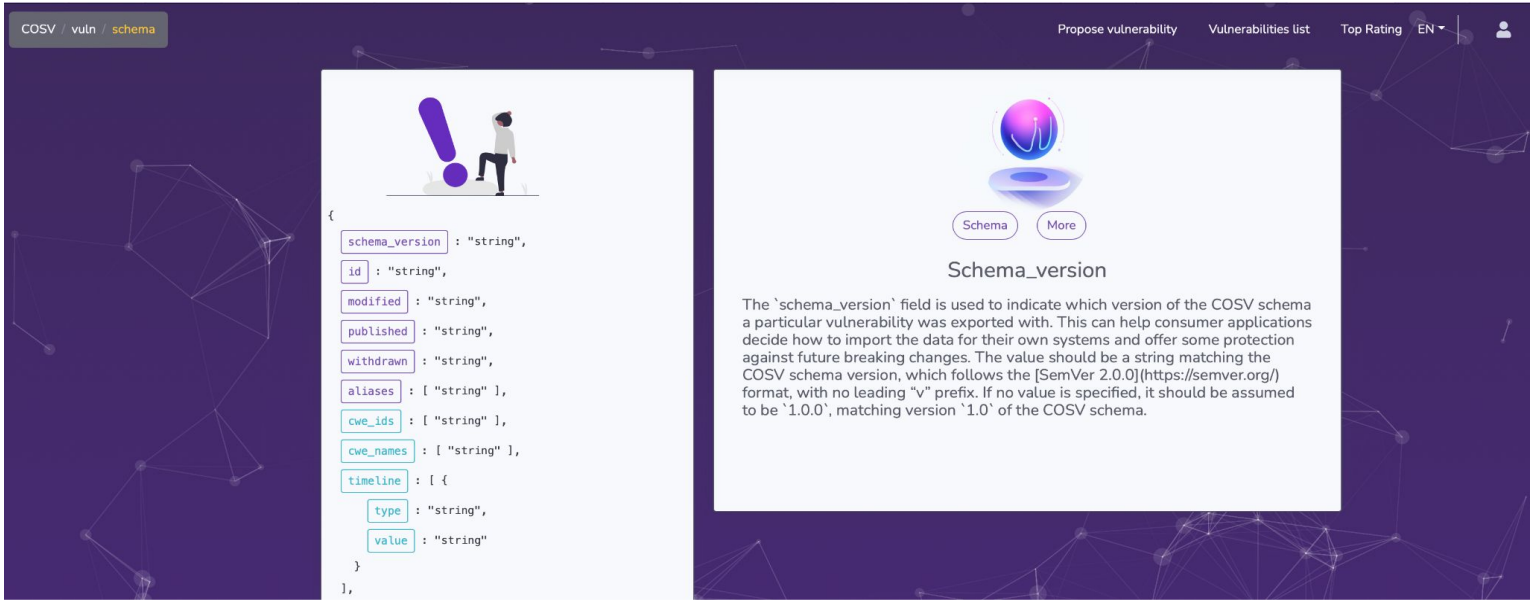
2023/06

Релиз версии 1.0.0

2023/07

HUAWEI 棱镜七彩 中国软件评测中心 奇安信 中国科学院软件所 中国科学院战略咨询研究院 电子五所 北京航空航天大学

Сама COSV схема: v1.0.0



https://www.gitlink.org.cn/zone/CCF-ODC/source/7

https://cosv.gitlink.org.cn/vuln/schema

Java/Kotlin Десериализаторы схемы: COSV4K

https://github.com/saveourtool/cosv4k

Patch details problems #8

Open akuleshov7 opened this issue on Aug 30, 2023 · 7 comments

akuleshov7 commented on Aug 30, 2023 — Member

1. `patches_detail[]` is now added as a separate field on the same level as `affected[]:` . It is incorrect, because we cannot make a mapping from an AFFECTED PROJECT (affected[]) to a patch where it was fixed and cannot properly show it.

Imagine, that your library XXX has two major versions 1.0.0 and 3.0.0 (both are supported).
Vulnerability fixes usually go into both version, and in COSV we say:

```
"ranges": [ {
    "type": "SEMVER",
    "events": [
      { "introduced": "1.0.0" },
      { "fixed": "1.0.2" },
      { "introduced": "3.0.0" },
      { "fixed": "3.2.5" }
    ]
} ]
```

And patches were different with different commits IDs. In current schema we cannot do anything and create mapping between those project and fix.

Suggestion to move `patches_detail` to `affected[].ranges[]` or `affected[]` . PLease think about that.

2. `affected[].package.language` is **DUPLICATED** with `patches_detail[].main_language`

JustinB1eber commented on Aug 30, 2023 • edited — Member

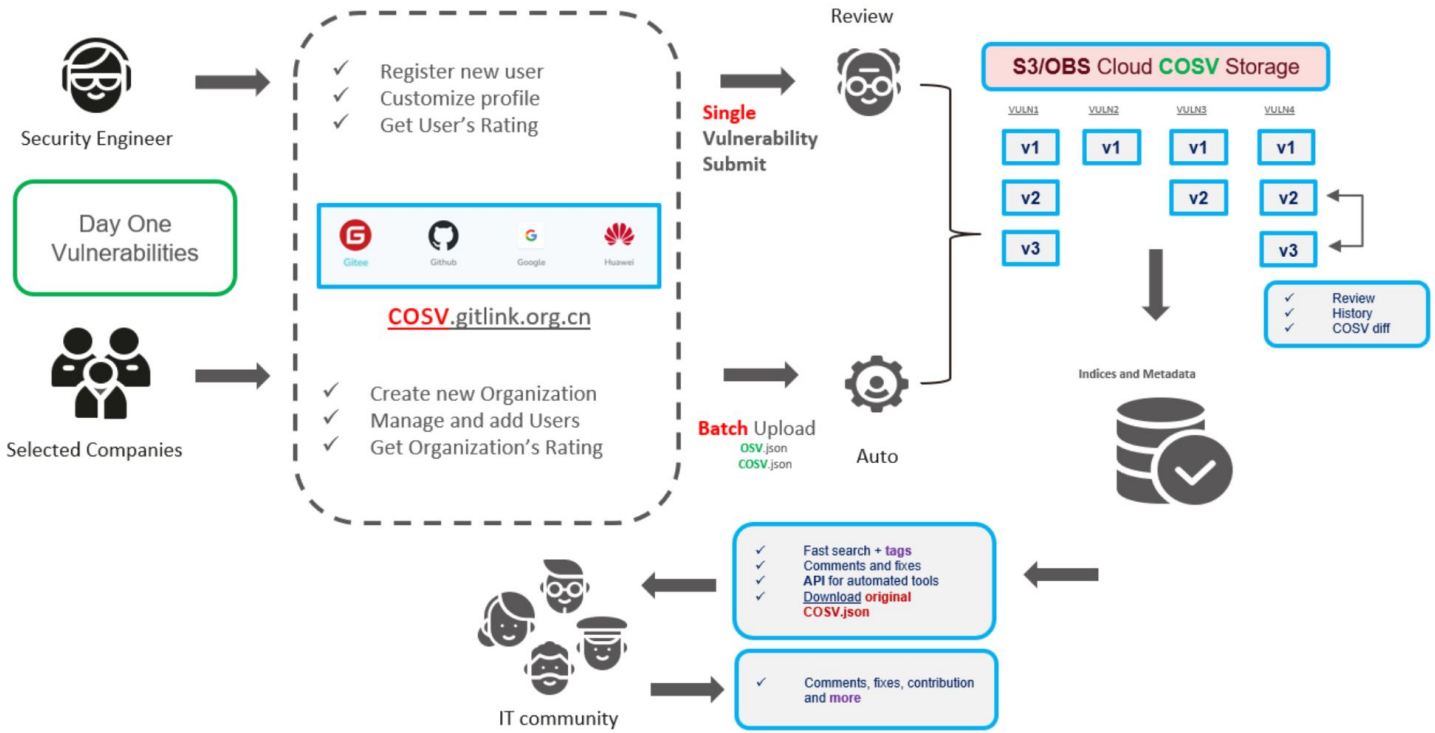
Thanks for your careful and considerate. Here's my opinions:

1. About `patches_detail[]` . At the beginning of the design, we hope that all data is a direct extension of the vulnerability, and the patch and the affected package use the vulnerability as a bridge to connect. But the problem you said exists.

- However, as far as the current vulnerability patch data situation is concerned, no vulnerability database provides a mapping between patches and specific fix versions on vulnerability reports. If we want to further correlate the patch to the affected version range based on the existing data, it may take a lot of time and cost.
- Once an accurate commit link as a patch is provided, with the code repository cloned, users can find out which branch the repair patch is applied to according to the git graph.
- If we want to associate the patch with the affected version range, we may need to modify the `affected[].package.ranges` field, and how to continue to be compatible with OSV would be a problem.

2. About `affected[].package.language` , it is used to indicate the major language of package is developed in. This may be mainly used to give classification labels when displaying vulnerability reports, but for users who use this package as a dependency, it has no clear effect. They don't care what language the dependent package is developed in. `patches_detail[].main_language` is a more precise field, and it has more practical use. Most of the time, the repair of a patch involves code logic changes, common in code languages such as Java and C++, and sometimes only involves modification of configuration files, such as xml. For example, for those researchers who use fixing patch as dataset to train vulnerability-related deep learning models, this field would be important.

COSV (да и любой другой) архив



Propose a new vulnerability

Upload COSV files

Vulnerability identifier*

Identifier...

Generate identifier

Summary*

Details*

Related link

https://example.com

Severity score vector*

3 | CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:N/A:N | +

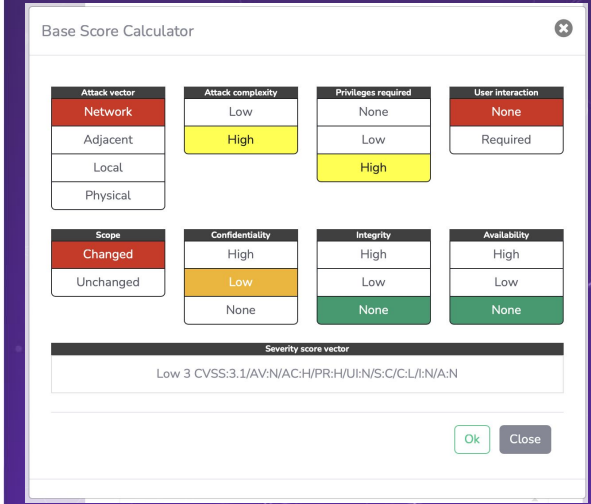
Organization

Collaborators

ak

acies312

Propose a vulnerability



Propose new

COSV / vuln / list

Propose vulnerability | Vulnerabilities list | Top Rating | EN | akuleshov7_1 User settings

Introducing

International Vulnerabilities Archive

Current page provides the list of publicly disclosed information security vulnerabilities and exposures.

New vulnerability

You can propose your own new vulnerability, if you didn't find it one in our list. After the review and approval, it will appear in the database under a special identifier.

In case of any error feel free to contact us.

Top rating

For each approved and accepted vulnerability you will get rating points. Here you can see the top rating of users and organizations.

PUBLIC | OWNER

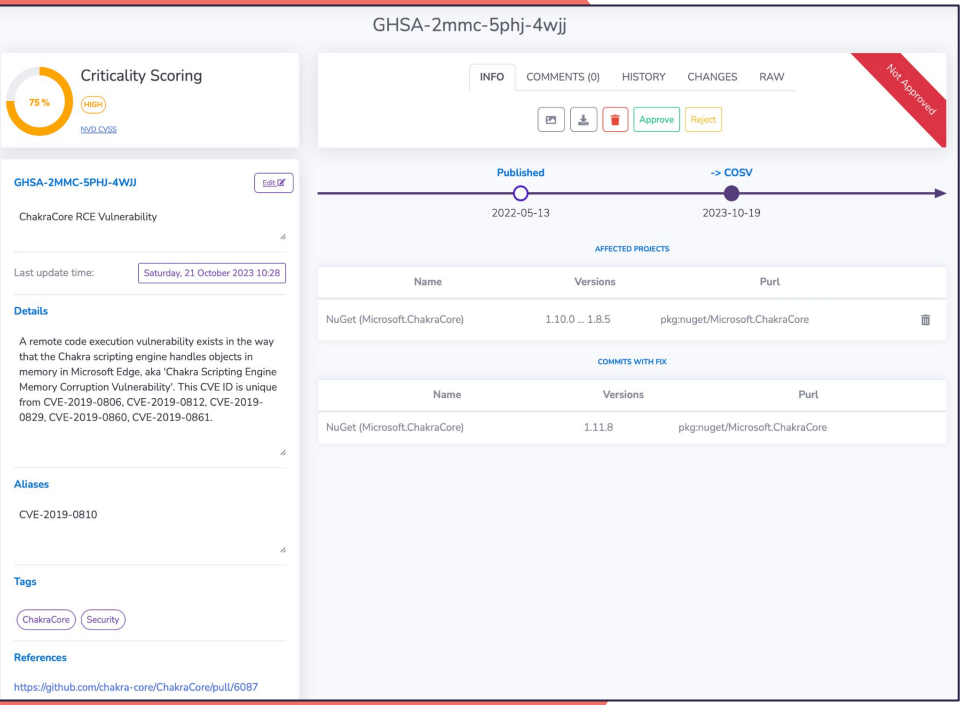
Identifier or Summary... | COSV Submitter... | Tag... | Language | Organization...

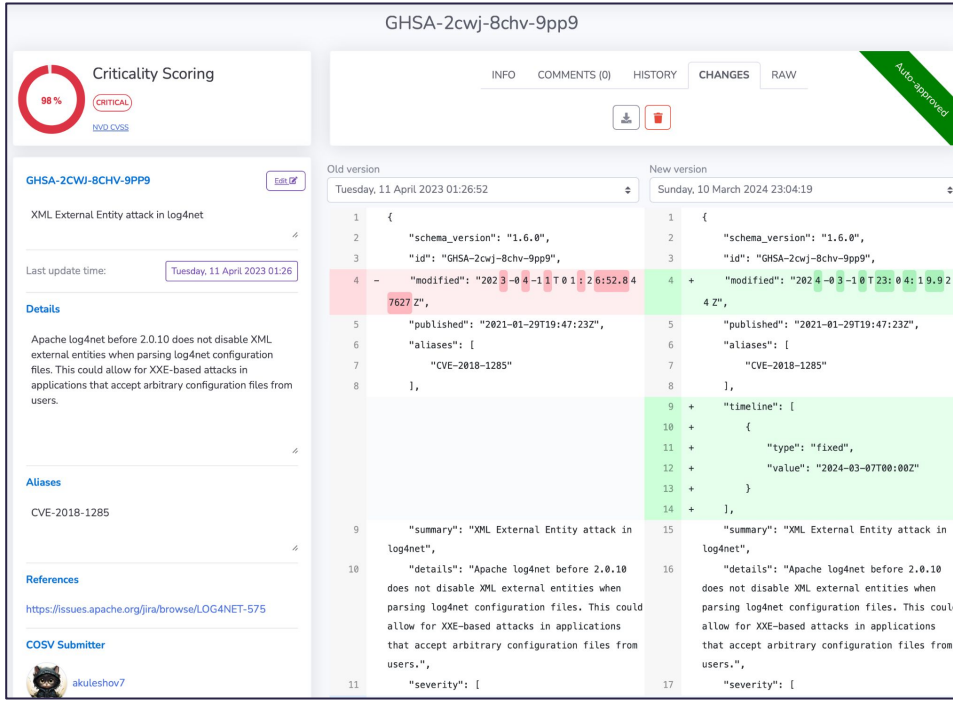
Identifier	Summary	Criticality	Language	COSV Submitter	Organization
GHSA-2m5h-6g38-jjf2	ChakraCore RCE Vulnerability	7.5	Other	akuleshov7	OSV
GHSA-2hp9-3xfr-r9w2	Insufficient token expiration in Serenity	7.8	Other	akuleshov7	OSV
GHSA-2c7v-qcjp-4mg2	.NET Remote Code Execution Vulnerability	8.8	Other	akuleshov7	OSV
GHSA-2pqj-h3vj-pqgw	Cross-Site Scripting in jquery	6.1	Other	akuleshov7	OSV
GHSA-2cwj-8chv-9pp9	XML External Entity attack in log4net	9.8	Other	akuleshov7	OSV
GHSA-2rfj-2mwp-787v	Out-of-bounds write	7.5	Other	akuleshov7	OSV
GHSA-2rvx-cvfc-mcp2	New Relic .NET Agent contains SQL Injection	9.8	Other	akuleshov7	OSV

« ‹ 1 2 3 › » Jump to the page → Show 7 entries

Page 1 of 9272

Агрегация/поиск





Страница уязвимости

akuleshov7

Andrey Kuleshov

RATING

2392

Customize profile

About

Kotlin Opensource Enthusiast, Software Engineer at Huawei

Huawei

Netherlands

akuleshov7

akuleshov7.com

Organizations

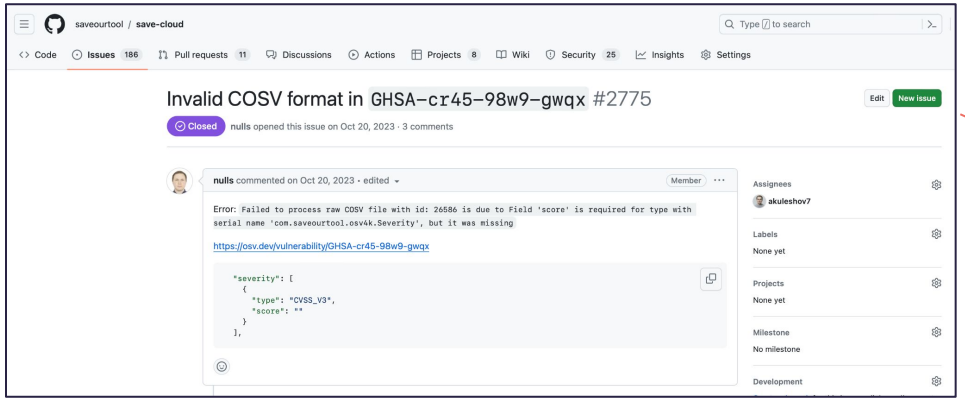
Identifier or Summary... | COSV Submitter... | Tag... | Language | Status | Organization...

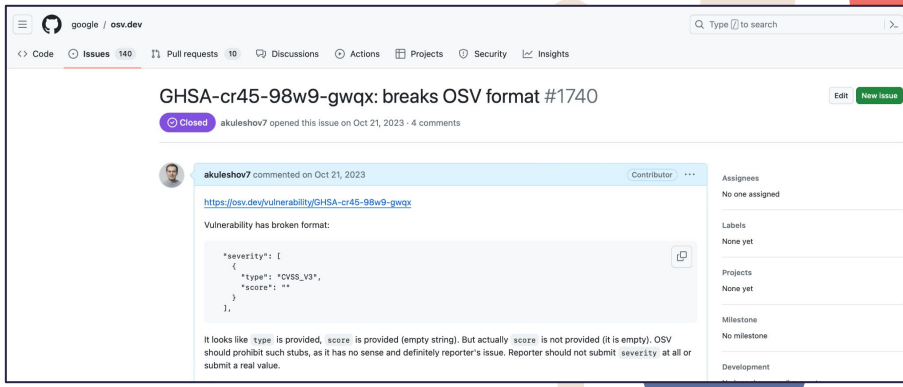
Add new vulnerability from json

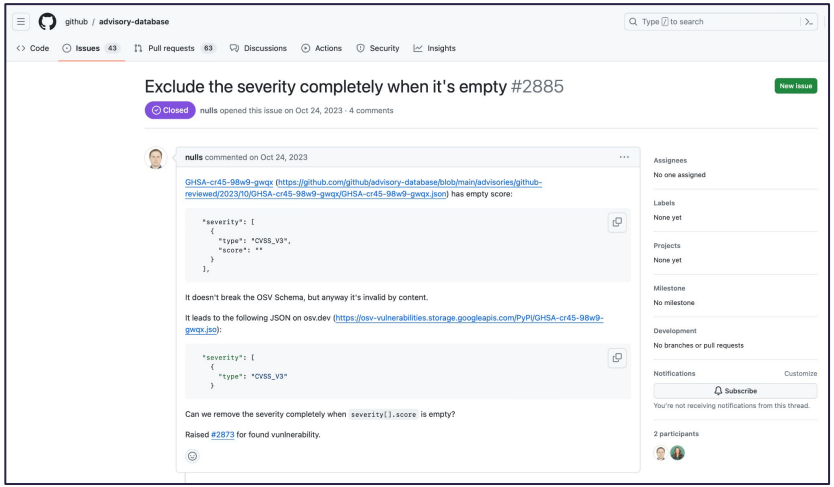
Identifier	Summary	Criticality	Language	Organization	Status
GHSA-2qgv-2cv4-g4cg ChakraCore	Out-of-bounds write in ChakraCore test test	7.5	Other	OSV	Rejected
GHSA-2mmc-5phj-4wjj ChakraCore Security	ChakraCore RCE Vulnerability	7.5	Other	OSV	Edited
GHSA-2m5h-6g38-jjf2	ChakraCore RCE Vulnerability	7.5	Other	OSV	Approved
GHSA-2hp9-3xfr-r9w2	Insufficient token expiration in Serenity	7.8	Other	OSV	Approved
GHSA-2c7v-qcjp-4mg2	.NET Remote Code Execution Vulnerability	8.8	Other	OSV	Approved
GHSA-2pqj-h3vj-pqgw	Cross-Site Scripting in jquery	6.1	Other	OSV	Approved
GHSA-2cwj-8chv-9pp9	XML External Entity attack in log4net	9.8	Other	OSV	Edited
GHSA-2rfj-2mwp-787v	Out-of-bounds write	7.5	Other	OSV	Approved
GHSA-2rvx-cvfc-mcp2	New Relic .NET Agent contains SQL Injection	9.8	Other	OSV	Approved
GHSA-2m65-m22p-9wjw	.NET Information Disclosure Vulnerability	5.9	Other	OSV	Approved

Завершая приготовление

Забавные вещи из бардака







Выводы

Форматы

Форматов и организаций бесчисленное количество, следим за CWE, CVE, OSV, GH

Свои архивы

Только если: *Партия сказала: надо! Комсомол ответил: есть!*

Лучше пишем сканеры

Возможности

Безграничные возможности: от bounty hunting для CodeQL до импортозамещения

Thanks!

Andrey Kuleshov

Tg: @akuleshov7
GH: @akuleshov7