広範な脆弱性情報の統合管理と履歴追跡

Norihiro Nakaoka, Shunichi Shinohara
@ CSS 2025 2F3-4

whoami

Norihiro Nakaoka / @MaineK00n

Future Corporation, Cyber Security Innovation Group
OSS Vulnerability Scanner: Vuls[1] Committer

[1] https://github.com/future-architect/vuls

論文・スライドPDF、デモを詳しく

https://github.com/vulsio/css2025-vuls2

Contents

1. なぜ脆弱性情報に「基盤」と「統合」、「履歴」が必要？
2. 提案手法と評価
3. 今後の課題

1. なぜ脆弱性情報に「基盤」と「統合」、「履歴」が必要？

脆弱性情報の更新遅延

脆弱性検知の観点から、脆弱性情報の更新は次の問題†を抱えている

- NVD更新遅延
- 一次データソースの更新がMITRE CVE/NVD/JVNへ反映されない

検知精度を向上するためには、一次データソースを取り扱わなければならない
取り扱う一次データソースが増えると、次の問題が発生する

- 安定してデータ取得することが難しい
- 新たなデータフォーマットの取り扱い

これらを解決するために、「基盤」「統合」が必要である

† Appendix A. にて、一次データソースとMITRE CVE/NVD/JVNの比較、NVD更新遅延の状況を解説

脆弱性情報を記述する多様なフォーマット

機械的に読むとして、脆弱性情報は多様なフォーマットで書かれている

例えば……
Red Hat: OVAL、CVRF、CSAF/CSAF VEX、OSV、CVE API
Ubuntu: OVAL、OpenVEX、OSV、CVE API、USN API、CVE Tracker

脆弱性情報が、多様なフォーマットで提供されると、次の問題†が発生する

- フォーマットごとに表現のしやすい情報が異なり、比較が大変
- 規格化されていても、ベンダ×フォーマットの読み方が必要

ベンダ、フォーマットを超えて、脆弱性情報を「統合」する必要がある

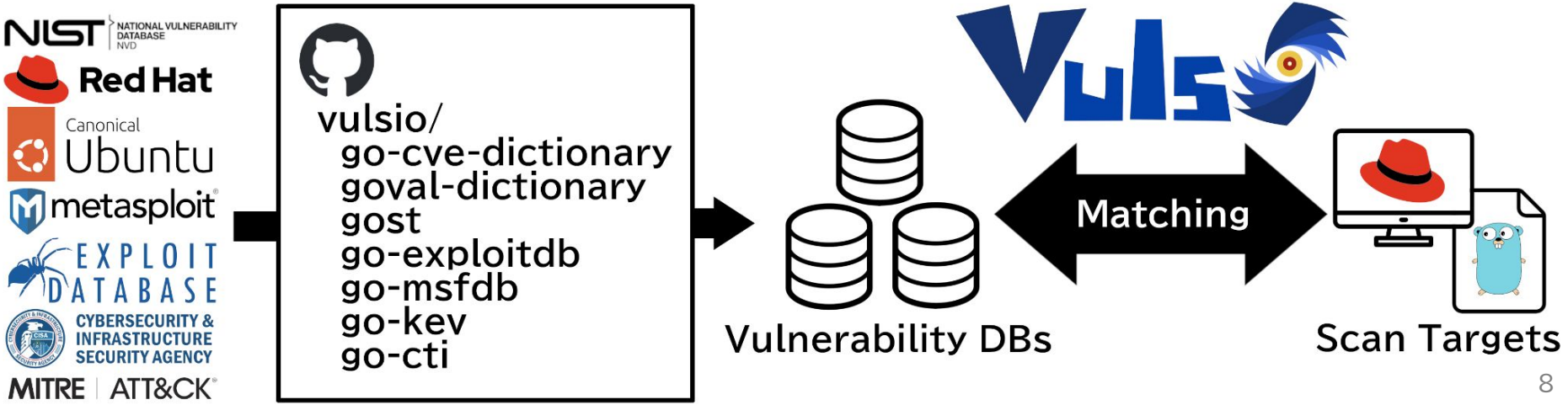
† Appendix B. にて、フォーマットの読み方を紹介、およびフォーマットごとに異なる情報問題を解説

以前までのVuls検知アーキテクチャの問題

検知結果を再現したり、差分を説明するには……

検知に使ったDBか、DBを作成したときのデータが必要だが、管理していない問題

データを「基盤」と「履歴」付きで管理することで再現可能に

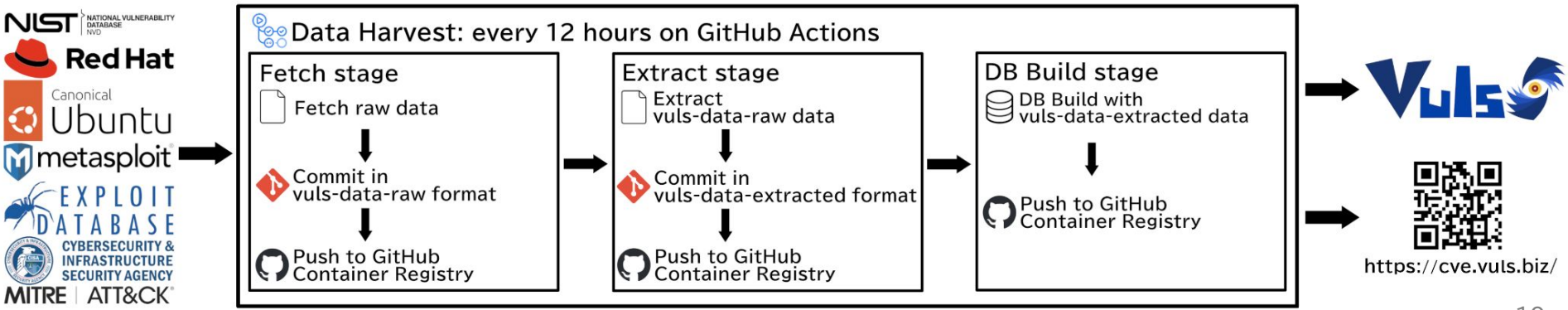


2. 提案手法と評価

提案手法: データハーベスト

Fetch, Extract, DB Buildの3ステージからなるデータハーベスト基盤を設計

- Fetch: 一次データソースをvuls-data-raw formatに変換、gitで管理
- Extract: vuls-data-raw dataを
  vuls-data-extracted formatで統合、gitで管理
- DB Build: vuls-data-extracted dataでDBを作成



評価(1): 広範なデータ収集と統合フォーマット

- 実装を行い OSS Vuls に組み込み、すでに実運用されている
  - raw, extracted データとデータベースは履歴付きでパブリックに公開
  - データハーベスト一連の処理は CI にて 12 時間おきに自動実行
  - データの鮮度確保と履歴管理を実現
- 広範な一次データソースの収集
  - raw として 173 種類、extracted として 25 種類をカバー
- 統合されたデータフォーマットの実現
  - Red Hat CSAF/CSAF VEX や Ubuntu CVE Tracker などの元データを統合されたフォーマットとセマンティクスに変換
  - 単独のデータ読み取りが容易になると同時に、データソース間の比較コストも削減

統合フォーマット解説(1/3)：全体構造 前半

Red Hat CSAF VEX の CVE-2024-43420.json を例にとる

```
{
    "id": "CVE-2024-43420",
    "advisories": [{
            "content": { "id": "RHBA-2025:9433" }
        }],
    "vulnerabilities": [{
            "content": {
                "id": "CVE-2024-43420",
                "title": "microcode_ctl: Exposure of sensitive information",
                "severity": [{
                        "type": "cvss_v31",
                        "source": "secalert@redhat.com",
                        "cvss_v31": {
                            "vector": "CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N"
                            ...
```

識別ID

アドバイザリ群

脆弱性の情報群

統合フォーマット解説(2/3): 全体構造 後半

```
    "detections": [
        {
            "ecosystem": "redhat:9",
            "conditions": [
                {
                    "criteria": { ... }
                }
            ]
        }
    ],
    "data_source": {
        "raws": [
            "vuls-data-raw-redhat-repository-to-cpe/repository-to-cpe.json",
            "vuls-data-raw-redhat-vex/2024/CVE-2024-43420.json"
        ]
    }
}
```

検知条件群

エコシステム

検知条件: 次のスライドで

このファイル生成に用いた raw のパス

統合フォーマット解説(3/3): 検知条件

```
{
    "type": "version",
    "version": {
        "vulnerable": true,
        "fix_status": { "class": "fixed" },
        "package": {
            "type": "binary",
            "binary": { "name": "microcode_ctl" }
        },
        "affected": {
            "type": "rpm",
            "range": [{ "lt": "4:20250211-1.20250512.1.el9_6" }]
        }
    }
}
```

種別:バージョンでの検知条件

修正状態: ここでは修正済み

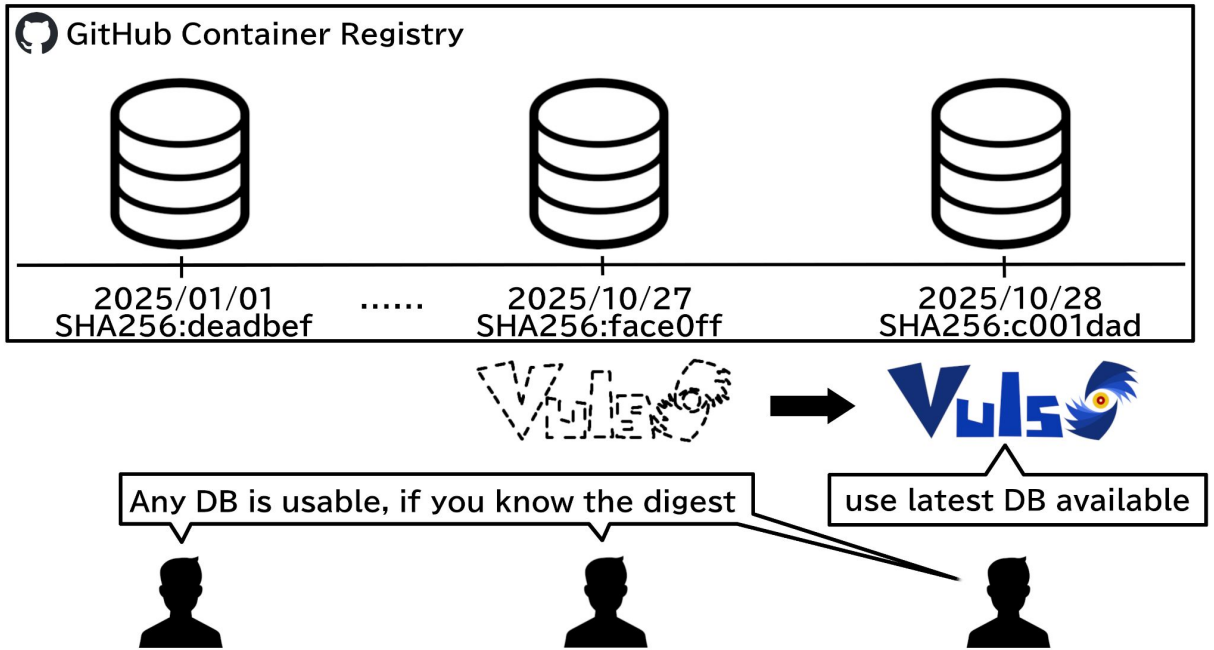
パッケージ種別: ここではバイナリパッケージ

パッケージ名

影響範囲:
RPM version として
less than で範囲指定

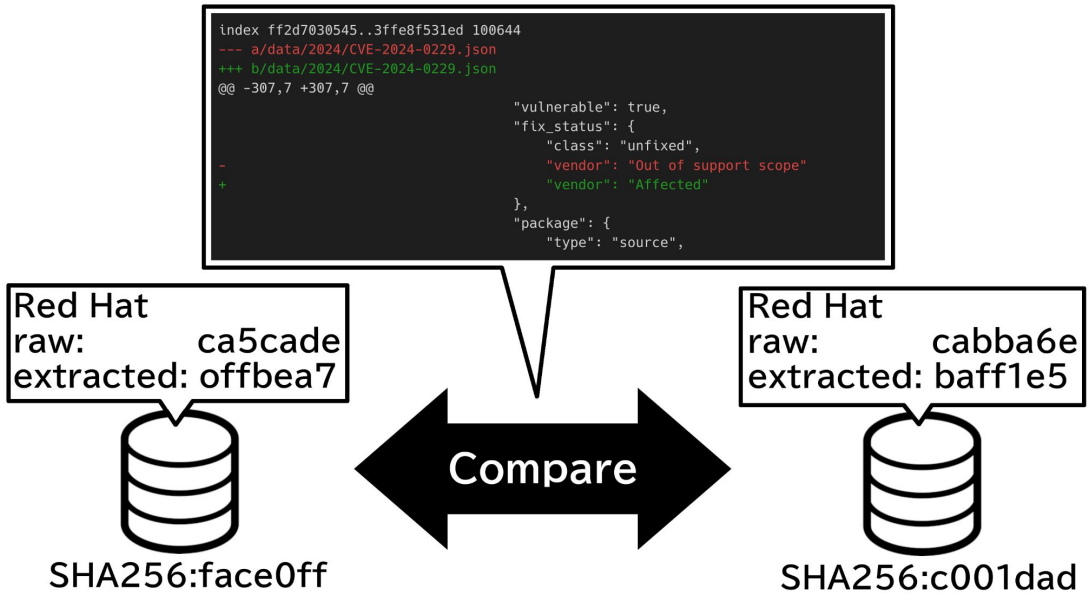
評価(2): 検知結果の再現性

データベースは、基本的に最新を使うが、ダイジェストで過去分も利用可能
⇒過去・他ユーザの検知環境を再現可能に



評価(3): 差分の説明性†

データベースは、使用したデータソースのcommit hashを保持
2つのDB間において、DB, extracted, rawの3段階で比較可能に



† Appendix C. にて、実際の差分を3パターン紹介

3. 今後の課題

データベースのサイズの最適化

- 配布の観点からはデータサイズをなるべく小さくしたい
  - 元の脆弱性情報がギガバイト超
  - 2025-10-28 zstd圧縮 0.03GiB / 伸長後 1.73 GiB
- 案1: 格納するフォーマットの変更
  - JSON ➔ ProtocolBuffers へ変更
  - カラム型フォーマットの利用（例: Parquet）
- 案2: データベース内部での圧縮
  - LSM-Tree でページ単位の圧縮を利用
  - SQLite3 でもプラグインによる圧縮機能あり

差分の論理的な説明能力の向上

- 現状の差分は JSON テキストのシンプルな diff
- 重要な変更(severity、fix status)も軽微な変更(更新日付)もおなじ重みで出てきてしまう
- 重要な変更だけを抽出したり、目立たせたい
  - 差分調査のコストを大きく下げる
- より論理的に差分を見る方法を見つけ出す必要あり

データハーベストの安定

- 取得元のサーバが遅い、応答しないなどのエラーが発生している
- 仕様変更によって取得処理がエラーとなることもある
  - この場合は取得/変換処理を修正するまで更新が停止
- パイプラインの安定性は, 鮮度と信頼性を直接的に左右
  - 継続的な改善が必要
- 安定化のために
  - リトライ機構の強化
  - エラー発生時の自動通知と復旧プロセスの改善
  - 元データの変更に対する柔軟な対応メカニズムの導入

論文・スライドPDF、
デモを詳しく

おわりに

脆弱性情報の更新遅延やフォーマットの多様さにより
生データをそれぞれ取り扱うことは困難
→「基盤」「統合」が必要

検知結果の変化を説明するには
脆弱性情報の変化を説明できなければならない
→「履歴」が必要

「統合」「履歴」を満たすデータハーベスト「基盤」を実装・評価

Appendix

Appendix A. 脆弱性情報の更新遅延

Fortinet vs MITRE CVE/NVD/JVN
FG-IR-22-455(CVE-2023-26207)

Fortinet VS MITRE CVE

Summary

An insertion of sensitive information into log file vulnerability [CWE-532] in FortiOS / FortiProxy log events may allow a remote authenticated attacker to read certain passwords in ciphertext.

Version	Affected	Solution
FortiOS 7.4	Not affected	Not Applicable
FortiOS 7.2	7.2.0 through 7.2.5	Upgrade to 7.2.6 or above
FortiOS 7.0	7.0.0 through 7.0.15	Upgrade to 7.0.16 or above
FortiOS 6.4	6.4 all versions	Migrate to a fixed release
FortiOS 6.2	6.2 all versions	Migrate to a fixed release
FortiOS 6.0	6.0 all versions	Migrate to a fixed release
FortiProxy 7.2	7.2.0 through 7.2.1	Upgrade to 7.2.2 or above
FortiProxy 7.0	7.0.0 through 7.0.7	Upgrade to 7.0.8 or above
FortiProxy 2.0	2.0.0 through 2.0.12	Upgrade to 2.0.13 or above
FortiProxy 1.2	Not affected	Not Applicable
FortiProxy 1.1	Not affected	Not Applicable

Follow the recommended upgrade path using our tool at: https://docs.fortinet.com/upgrade-tool

IR Number	FG-IR-22-455
Published Date	Jun 12, 2023
Updated Date	Oct 22, 2024
Component	CLI
Severity	⚠ Low
CVSSv3 Score	3.3
Impact	Information disclosure
CVE ID	CVE-2023-26207

Product Status

Learn more

Fortinet — FortiProxy

Versions 2 Total

Default Status: *unaffected*

Affected

- affected from 7.2.0 through 7.2.1
- affected from 7.0.0 through 7.0.10

Vendor	Product
Fortinet	FortiOS

Versions 1 Total

Default Status: *unaffected*

Affected

- affected from 7.2.0 through 7.2.5

https://www.fortiguard.com/psirt/FG-IR-22-455
https://www.cve.org/CVERecord?id=CVE-2023-26207

Fortinet VS NVD

Summary

An insertion of sensitive information into log file vulnerability [CWE-532] in FortiOS / FortiProxy log events may allow a remote authenticated attacker to read certain passwords in ciphertext.

Version	Affected	Solution
FortiOS 7.4	Not affected	Not Applicable
FortiOS 7.2	7.2.0 through 7.2.5	Upgrade to 7.2.6 or above
FortiOS 7.0	7.0.0 through 7.0.15	Upgrade to 7.0.16 or above
FortiOS 6.4	6.4 all versions	Migrate to a fixed release
FortiOS 6.2	6.2 all versions	Migrate to a fixed release
FortiOS 6.0	6.0 all versions	Migrate to a fixed release
FortiProxy 7.2	7.2.0 through 7.2.1	Upgrade to 7.2.2 or above
FortiProxy 7.0	7.0.0 through 7.0.7	Upgrade to 7.0.8 or above
FortiProxy 2.0	2.0.0 through 2.0.12	Upgrade to 2.0.13 or above
FortiProxy 1.2	Not affected	Not Applicable
FortiProxy 1.1	Not affected	Not Applicable

Follow the recommended upgrade path using our tool at: https://docs.fortinet.com/upgrade-tool

IR Number	FG-IR-22-455
Published Date	Jun 12, 2023
Updated Date	Oct 22, 2024
Component	CLI
Severity	⚠ Low
CVSSv3 Score	3.3
Impact	Information disclosure
CVE ID	CVE-2023-26207

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:* Show Matching CPE(s)	From (including) 7.0.0	Up to (including) 7.0.10
cpe:2.3:a:fortinet:fortiproxy:7.2.0:*:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:fortinet:fortiproxy:7.2.1:*:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* Show Matching CPE(s)	From (including) 7.2.0	Up to (including) 7.2.4

https://www.fortiguard.com/psirt/FG-IR-22-455
https://nvd.nist.gov/vuln/detail/cve-2023-26207

Fortinet VS JVN

Summary

An insertion of sensitive information into log file vulnerability [CWE-532] in FortiOS / FortiProxy log events may allow a remote authenticated attacker to read certain passwords in ciphertext.

Version	Affected	Solution
FortiOS 7.4	Not affected	Not Applicable
FortiOS 7.2	7.2.0 through 7.2.5	Upgrade to 7.2.6 or above
FortiOS 7.0	7.0.0 through 7.0.15	Upgrade to 7.0.16 or above
FortiOS 6.4	6.4 all versions	Migrate to a fixed release
FortiOS 6.2	6.2 all versions	Migrate to a fixed release
FortiOS 6.0	6.0 all versions	Migrate to a fixed release
FortiProxy 7.2	7.2.0 through 7.2.1	Upgrade to 7.2.2 or above
FortiProxy 7.0	7.0.0 through 7.0.7	Upgrade to 7.0.8 or above
FortiProxy 2.0	2.0.0 through 2.0.12	Upgrade to 2.0.13 or above
FortiProxy 1.2	Not affected	Not Applicable
FortiProxy 1.1	Not affected	Not Applicable

Follow the recommended upgrade path using our tool at: https://docs.fortinet.com/upgrade-tool

IR Number	FG-IR-22-455
Published Date	Jun 12, 2023
Updated Date	Oct 22, 2024
Component	CLI
Severity	⚠ Low
CVSSv3 Score	3.3
Impact	Information disclosure
CVE ID	CVE-2023-26207

影響を受けるシステム

フォーティネット

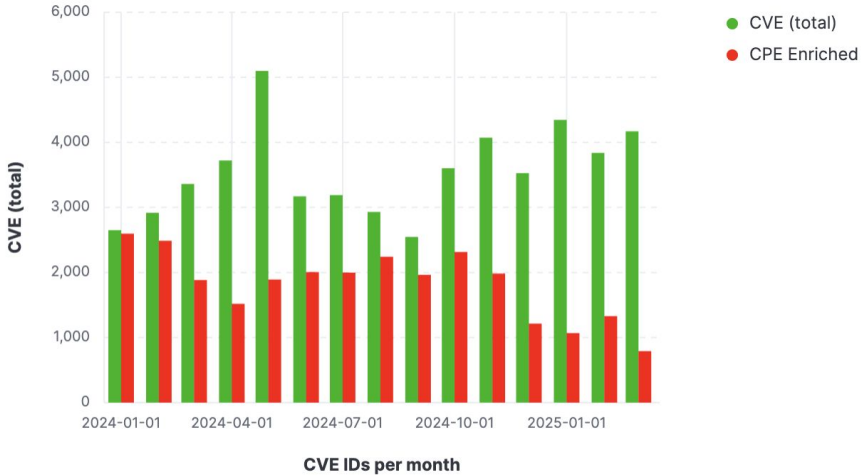
- FortiProxy 7.0.0 から 7.0.10
- FortiProxy 7.2.0
- FortiProxy 7.2.1
- FortiOS 7.2.0 から 7.2.4

https://www.fortiguard.com/psirt/FG-IR-22-455
https://jvndb.jvn.jp/ja/contents/2023/JVNDB-2023-022757.html

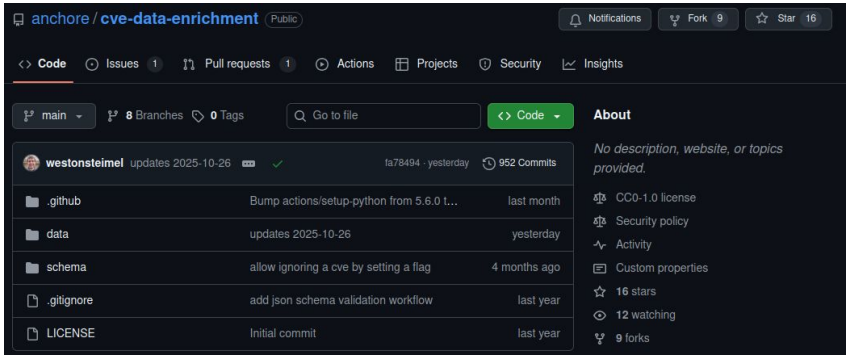
NVD更新遅延問題

NVD更新遅延問題

2024年3月ぐらいから
脆弱性情報の解析が遅れていた.
Anchore社は独自にEnrichment
を行い、公開している[1][2]



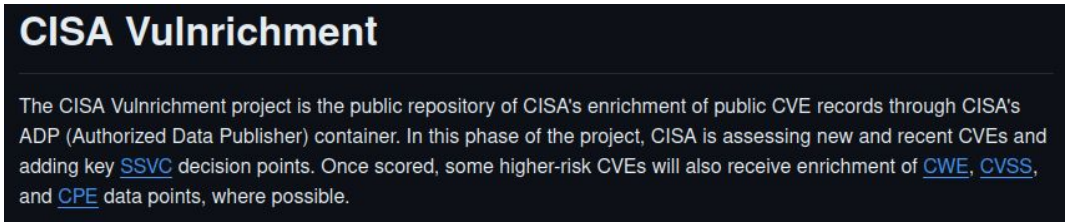
2025-10-24時点でNVDによる
解析待ちは26429件ある[3]



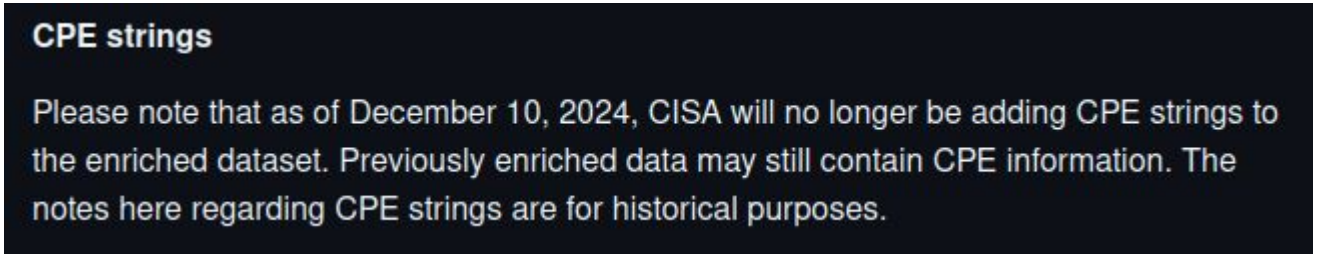
[1] https://anchore.com/blog/nvd-crisis-one-year-later/
[2] https://github.com/anchore/cve-data-enrichment
[3] https://nvd.nist.gov/general/nvd-dashboard

CISA Vulnrichment

2024年5月8日 CISA Vulnrichment が発表され、
CPEなどEnrichmentしてくれるように



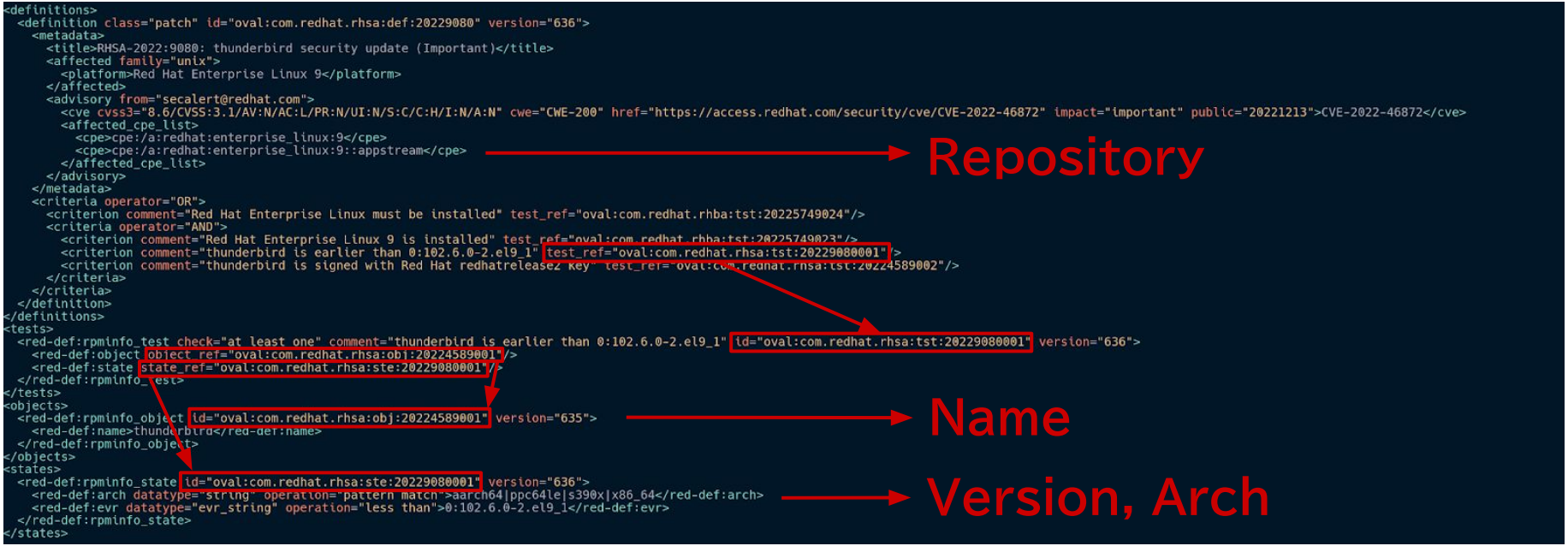
しかし、2024年12月10日、CPEのEnrichmentが停止



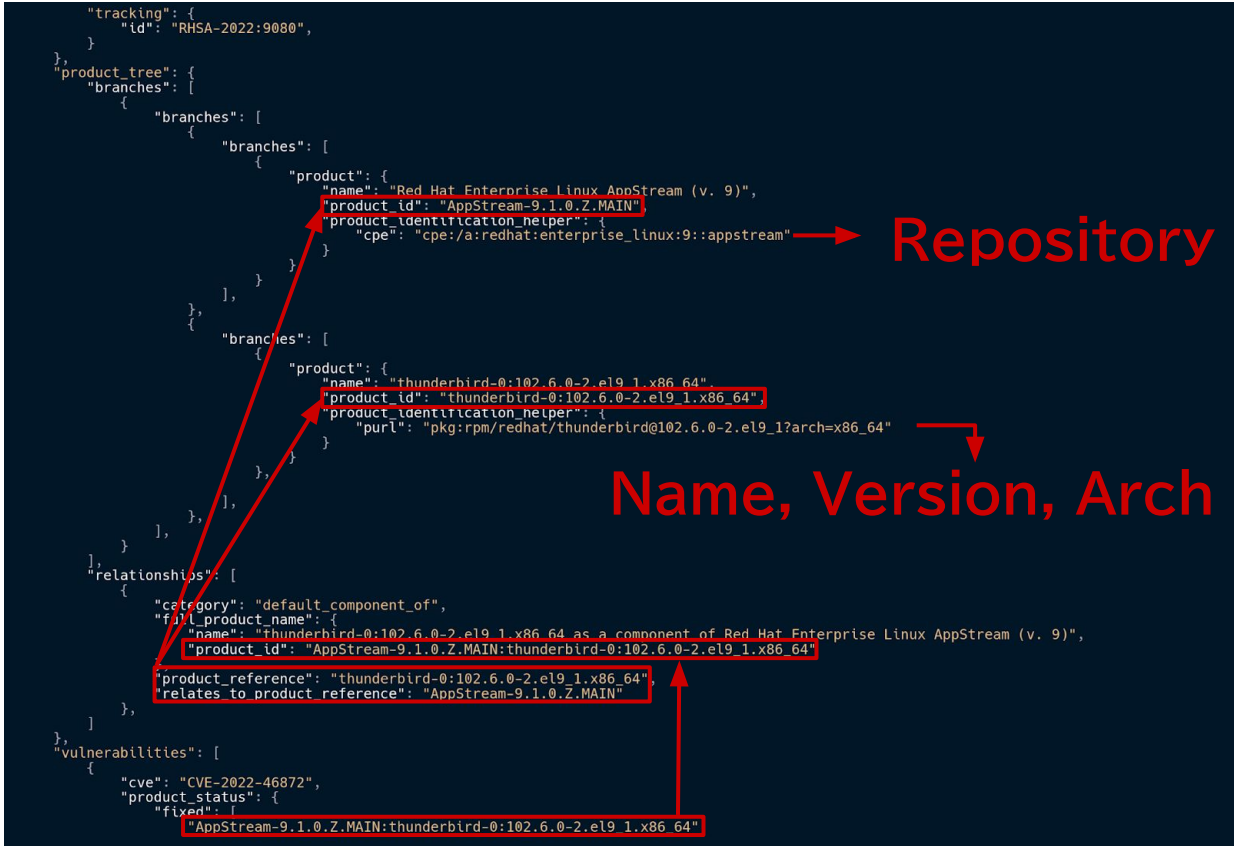
Appendix B.
脆弱性情報を記述する多様なフォーマット

フォーマット紹介

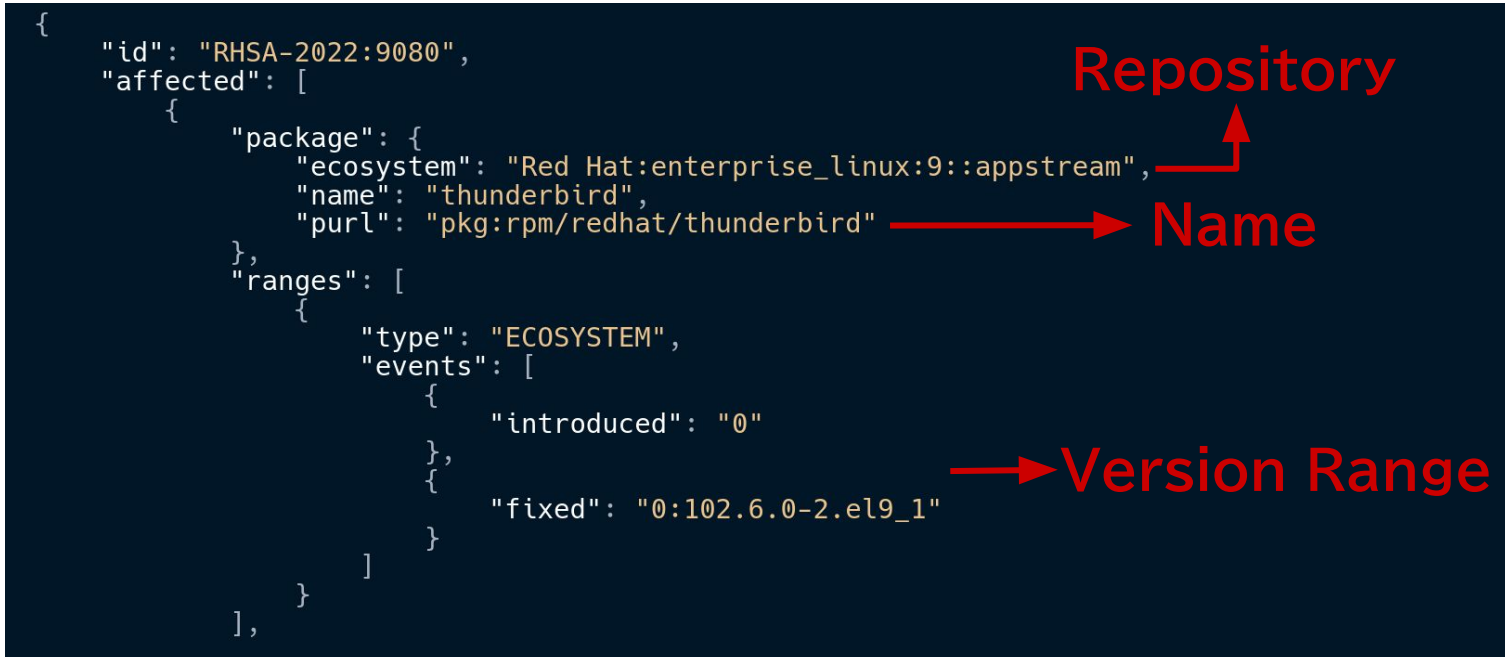
Red Hat OVAL: RHSA-2022:9080



Red Hat CSAF: RHSA-2022:9080



Red Hat OSV: RHSA-2022:9080

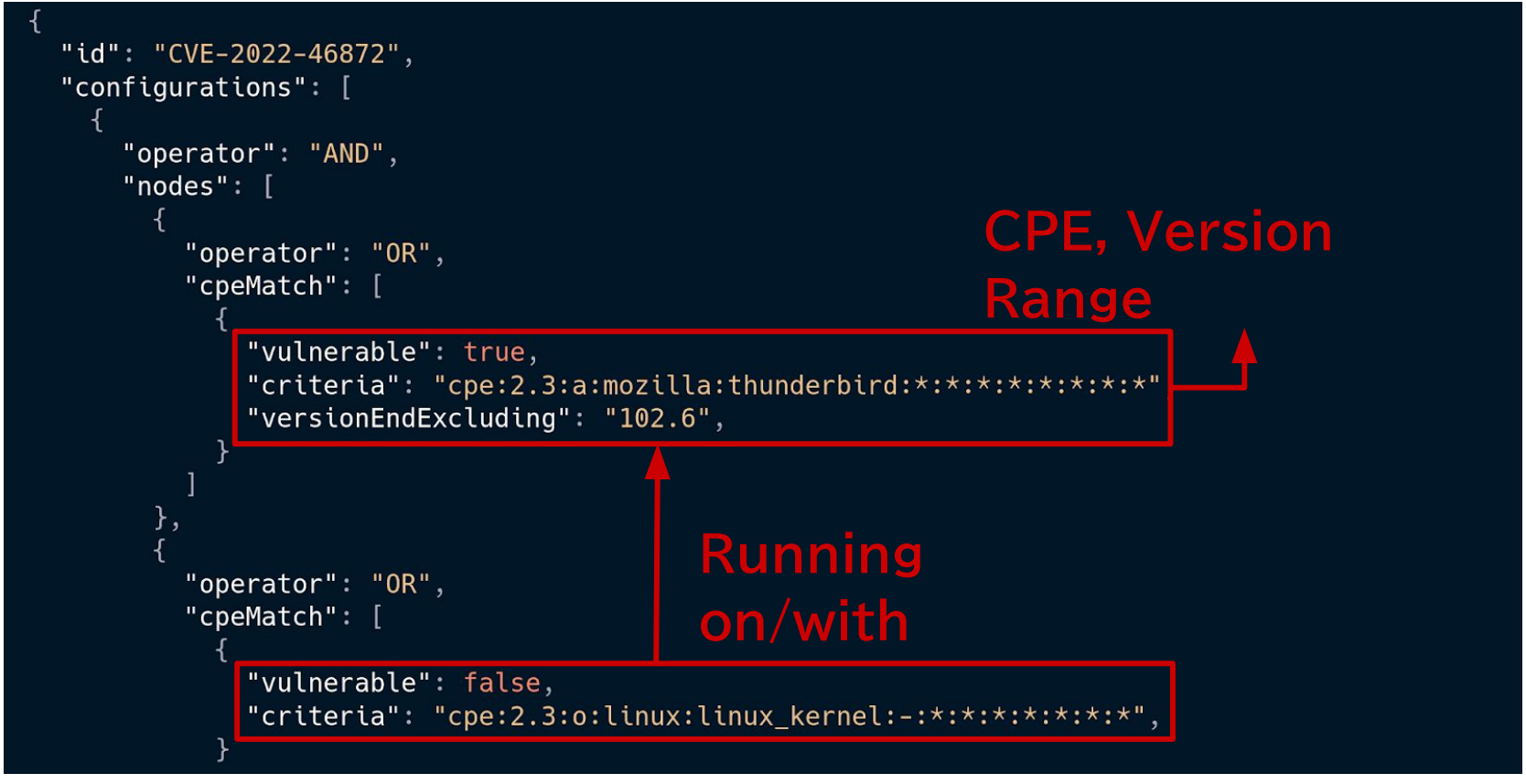


Red Hat CVE API: CVE-2022-46872


```
{
  "name": "CVE-2022-46872",
  "affected_release": [
    {
      "product_name": "Red Hat Enterprise Linux 9",
      "release_date": "2022-12-15T00:00:00Z",
      "advisory": "RHSA-2022:9080",
      "cpe": "cpe:/a:redhat:enterprise_linux:9",
      "package": "thunderbird-0:102.6.0-2.el9_1"
    },
```


→ Name, Version

NVD Feed: CVE-2022-46872



MITRE CVE v5: CVE-2022-46872

フォーマットごとに脆弱性情報が異なる問題

CVE-2021-47378: OVAL vs CVE API

```
<definition class="vulnerability" id="oval:com.redhat.cve:def:202147378" version="636">
      <metadata>
        <title>kernel: nvme-rdma: destroy cm id before destroy qp to avoid use after free (moderate)</title>
        <advisory from="secalert@redhat.com">
          <cve cvss3="6.0/CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:H" cwe="CWE-416" href="https://access.redhat.com/security/cve/
CVE-2021-47378" impact="moderate" public="20240521">CVE-2021-47378</cve>
          <affected>
            <resolution state="Affected">
              <component>kernel</component>
              <component>kernel-rt</component>
              <component>kernel-rt</component>
              <component>kernel-rt-core</component>
              <component>kernel-rt-core</component>
              ...
```

Affected or Will not fix ?

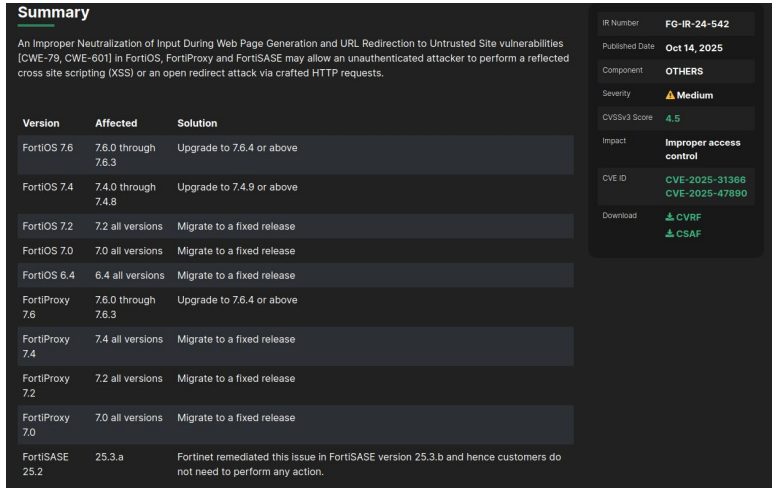
```
{
  "name" : "CVE-2021-47378",
  "bugzilla" : {
    "description" : "kernel: nvme-rdma: destroy cm id before destroy qp to avoid use after free",
    "id" : "2282362",
    "url" : "https://bugzilla.redhat.com/show_bug.cgi?id=2282362"
  },
  "package_state" : [ {
    "product_name" : "Red Hat Enterprise Linux 9",
    "fix_state" : "Will not fix",
    "package_name" : "kernel",
    "cpe" : "cpe:/o:redhat:enterprise_linux:9"
  }, {
    "product_name" : "Red Hat Enterprise Linux 9",
    "fix_state" : "Will not fix",
    "package_name" : "kernel-rt",
    "cpe" : "cpe:/o:redhat:enterprise_linux:9"
  }
  ...
```

Web: FG-IR-24-542

FortiSASE 25.3.a は

- CVE-2025-31366
- CVE-2025-47890

の影響を受ける



Summary

An Improper Neutralization of Input During Web Page Generation and URL Redirection to Untrusted Site vulnerabilities [CWE-79, CWE-601] in FortiOS, FortiProxy and FortiSASE may allow an unauthenticated attacker to perform a reflected cross site scripting (XSS) or an open redirect attack via crafted HTTP requests.

Version	Affected	Solution
FortiOS 7.6	7.6.0 through 7.6.3	Upgrade to 7.6.4 or above
FortiOS 7.4	7.4.0 through 7.4.8	Upgrade to 7.4.9 or above
FortiOS 7.2	7.2 all versions	Migrate to a fixed release
FortiOS 7.0	7.0 all versions	Migrate to a fixed release
FortiOS 6.4	6.4 all versions	Migrate to a fixed release
FortiProxy 7.6	7.6.0 through 7.6.3	Upgrade to 7.6.4 or above
FortiProxy 7.4	7.4 all versions	Migrate to a fixed release
FortiProxy 7.2	7.2 all versions	Migrate to a fixed release
FortiProxy 7.0	7.0 all versions	Migrate to a fixed release
FortiSASE 25.2	25.3.a	Fortinet remediated this issue in FortiSASE version 25.3.b and hence customers do not need to perform any action.

IR Number	FG-IR-24-542
Published Date	Oct 14, 2025
Component	OTHERS
Severity	Medium
CVSSv3 Score	4.5
Impact	Improper access control
CVE ID	CVE-2025-31366 CVE-2025-47890
Download	CVRF CSAF

https://www.fortiguard.com/psirt/FG-IR-24-542

CVRF: FG-IR-24-542

FortiSASE 25.2.a, 25.2.b は

- CVE-2025-31366
- CVE-2025-47890

の影響を受ける

FYI: CVRFの仕様では、
1つのVulnerabilityの中に
CVEは1つまでしか書けない

Fortinetが提供するCVRFは
仕様違反と思われる

```
    <cvrf:DocumentTracking>
        <cvrf:Identification>
            <cvrf:ID>FG-IR-24-542</cvrf:ID>
        </cvrf:Identification>
    </cvrf:DocumentTracking>
    <ProductTree>
        <Branch Name="Fortinet" Type="Vendor">
            ...
            <Branch Name="FortiSASE" Type="Product Name">
                <Branch Name="25.2.b" Type="Product Version">
                    <FullProductName ProductID="FortiSASE-25.2.b">FortiSASE 25.2.b</FullProductName>
                </Branch>
                <Branch Name="25.2.a" Type="Product Version">
                    <FullProductName ProductID="FortiSASE-25.2.a">FortiSASE 25.2.a</FullProductName>
                </Branch>
            </Branch>
        </Branch>
    </ProductTree>
    <Vulnerability Ordinal="1">
        <Title>Open Redirect and XSS in Web Filter warning page</Title>
        <cvrf:CVE>CVE-2025-31366</cvrf:CVE>
        <cvrf:CVE>CVE-2025-47890</cvrf:CVE>
        <ProductStatuses>
            <Status Type="Known Affected">
                ...
                <ProductID>FortiProxy-7.0.0</ProductID>
                <ProductID>FortiSASE-25.2.b</ProductID>
                <ProductID>FortiSASE-25.2.a</ProductID>
            </Status>
        </ProductStatuses>
```

6.8 Vulnerability – CVE

Element `vuln:CVE`

« The `vuln:CVE` element MUST be present zero or one time in any `vuln:Vulnerability` and if present its value holds the MITRE standard Common Vulnerabilities and Exposures (CVE) tracking number for the vulnerability and this value MUST match the pattern documented in section 2.2.10 Vulnerability CVE Type Model. » [CSAF-6.8-1]

Non-normative comment:

CVE is a standard for vulnerability naming that provides improved tracking of vulnerabilities over time across different reporting sources. More information about CVE domain values can be found in section 2.2.10 Vulnerability CVE Type Model.

Example 56:

```
<CVE>CVE-2010-3864</CVE>
```

https://www.fortiguard.com/psirt/cvrf/FG-IR-24-542
https://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/cs01/csaf-cvrf-v1.2-cs01.html#_Toc493508922

CSAF: FG-IR-24-542

CVE-IDは記述されていない
FortiSASE 25.2.a, 25.2.b が
影響を受ける

```
"product_tree": {
    "branches": [
        {
            "category": "vendor",
            "name": "Fortinet PSIRT",
            "branches": [
                {
                    "category": "product_name",
                    "name": "FortiSASE",
                    "branches": [
                        {
                            "category": "product_version",
                            "name": "FortiSASE 25.2.a",
                            "product": {
                                "name": "FortiSASE",
                                "product_id": "FortiSASE-25.2.a"
                            }
                        },
                        {
                            "category": "product_version",
                            "name": "FortiSASE 25.2.b",
                            "product": {
                                "name": "FortiSASE",
                                "product_id": "FortiSASE-25.2.b"
                            }
                        },
                        ...
                        {
                            "category": "product_version",
                            "name": "FortiSASE 24.4.a",
                            "product": {
                                "name": "FortiSASE",
                                "product_id": "FortiSASE-24.4.a"
                            }
                        },
                        {
                            "category": "product_version",
                            "name": "FortiSASE 25.2.b",
                            "product": {
                                "name": "FortiSASE",
                                "product_id": "FortiSASE-25.2.b"
                            }
                        },
                        {
                            "category": "product_version",
                            "name": "FortiSASE 25.3.b",
                            "product": {
                                "name": "FortiSASE",
                                "product_id": "FortiSASE-25.3.b"
                            }
                        }
                    ]
                }
            ]
        }
    ],
    "vulnerabilities": [
        {
            "title": "FortiSASE - Medium - FG-IR-24-542 - ADV: Open Redirect and XSS in Web Filter warning page",
            "product_status": {
                "known_affected": [
                    "FortiSASE-25.2.a",
                    "FortiSASE-25.2.b"
                ],
                "known_not_affected": [
                    "FortiSASE-22.4",
                    "FortiSASE-23.1",
                    "FortiSASE-23.1.1",
                    "FortiSASE-23.1.2",
                    "FortiSASE-23.1.3",
                    "FortiSASE-23.1.4",
                    "FortiSASE-23.1.a",
                    "FortiSASE-23.1.6",
                    "FortiSASE-23.1.7",
                    "FortiSASE-23.1.8",
                    "FortiSASE-23.1.9",
                    "FortiSASE-23.1.10",
                    "FortiSASE-23.1.11",
                    "FortiSASE-23.1.12",
                    "FortiSASE-23.1.13",
                    "FortiSASE-23.1.14",
                    "FortiSASE-23.1.15",
                    "FortiSASE-23.1.16",
                    "FortiSASE-23.1.17",
                    "FortiSASE-23.1.18",
                    "FortiSASE-23.1.19",
                    "FortiSASE-23.1.20",
                    "FortiSASE-23.1.b",
                    "FortiSASE-23.2",
                    "FortiSASE-23.2.a",
                    "FortiSASE-23.2.b",
                    "FortiSASE-23.3",
                    "FortiSASE-23.3.b",
                    "FortiSASE-23.3.2",
                    "FortiSASE-24.4.a",
                    "FortiSASE-25.2.b",
                    "FortiSASE-25.3.b"
                ]
            },
            "remediations": [
                {
                    "details": "FortiSASE 25.2: Fortinet remediated this issue in FortiSASE version 25.3.b and
hence customers do not need to perform any action.\n",
                    "category": "vendor_fix",
                    "product_ids": [
                        "FortiSASE"
                    ]
                }
            ]
```


https://www.fortiguard.com/psirt/csaf/FG-IR-24-542?csaf_url=https://filestore.fortinet.com/fortiguard/psirt/csaf_open-redirect-and-xss-in-web-filter-warning-page.json

Mail: FG-IR-24-542

CVE-2025-47890は
FortiSASE 25.2.bで修正

CVE-2025-31366は
FortiSASE 25.3.bで修正

Our PSIRT team replied to your question :
"

The advisory for FG-IR-24-542 is fixing multiple issues under the same vulnerability class, which is what caused the confusion.

In particular, the first CVE-2025-47890 is solved in FortiSASE 25.2.b (mantis # 1151911), while CVE-2025-31366 in FortiSASE version 25.3.b (mantis #1151910).

We are making sure to update the advisory CVRF accordingly.

Hope this clarifies.

"

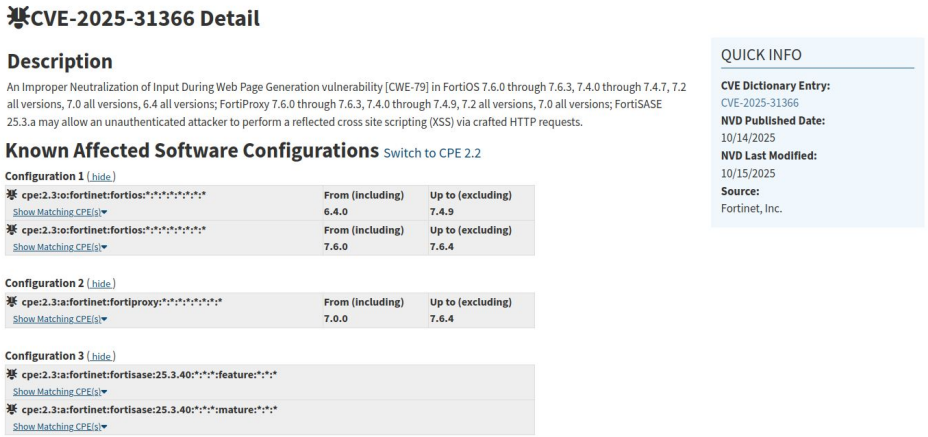
Thank you,

FortiGuard Team

NVD: CVE-2025-31366

Descriptionを読むと
Fortinet 25.3.a が影響を受ける

なぜか、CPEのversionは
25.3.40になっている



CVE-2025-31366 Detail

Description

An Improper Neutralization of Input During Web Page Generation vulnerability [CWE-79] in FortiOS 7.6.0 through 7.6.3, 7.4.0 through 7.4.7, 7.2 all versions, 7.0 all versions, 6.4 all versions; FortiProxy 7.6.0 through 7.6.3, 7.4.0 through 7.4.9, 7.2 all versions, 7.0 all versions; FortiSASE 25.3.a may allow an unauthenticated attacker to perform a reflected cross site scripting (XSS) via crafted HTTP requests.

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	6.4.0	7.4.9
cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	7.6.0	7.6.4

Configuration 2 (hide)

cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	7.0.0	7.6.4

Configuration 3 (hide)

cpe:2.3:a:fortinet:fortisase:25.3.40:*:*:feature:*:*
Show Matching CPE(s)
cpe:2.3:a:fortinet:fortisase:25.3.40:*:*:mature:*:*
Show Matching CPE(s)

QUICK INFO

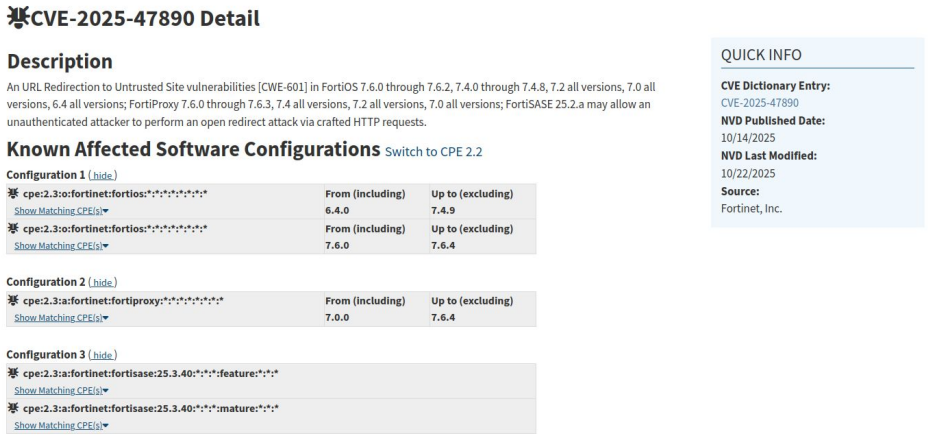
CVE Dictionary Entry:
CVE-2025-31366
NVD Published Date:
10/14/2025
NVD Last Modified:
10/15/2025
Source:
Fortinet, Inc.

https://nvd.nist.gov/vuln/detail/CVE-2025-31366

NVD: CVE-2025-47890

Descriptionを読むと
Fortinet 25.2.a が影響を受ける

CVE-2025-31366の
Descriptionに書いてある
バージョンは異なるにも関わらず
CPEは同じである



CVE-2025-47890 Detail

Description

An URL Redirection to Untrusted Site vulnerabilities [CWE-601] in FortiOS 7.6.0 through 7.6.2, 7.4.0 through 7.4.8, 7.2 all versions, 7.0 all versions, 6.4 all versions; FortiProxy 7.6.0 through 7.6.3, 7.4 all versions, 7.2 all versions, 7.0 all versions; FortiSASE 25.2.a may allow an unauthenticated attacker to perform an open redirect attack via crafted HTTP requests.

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	6.4.0	7.4.9
cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	7.6.0	7.6.4

Configuration 2 (hide)

cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	7.0.0	7.6.4

Configuration 3 (hide)

cpe:2.3:a:fortinet:fortisase:25.3.40:*:*:feature:*:*:*
Show Matching CPE(s)
cpe:2.3:a:fortinet:fortisase:25.3.40:*:*:mature:*:*:*
Show Matching CPE(s)

QUICK INFO

CVE Dictionary Entry:
CVE-2025-47890
NVD Published Date:
10/14/2025
NVD Last Modified:
10/22/2025
Source:
Fortinet, Inc.

https://nvd.nist.gov/vuln/detail/CVE-2025-47890

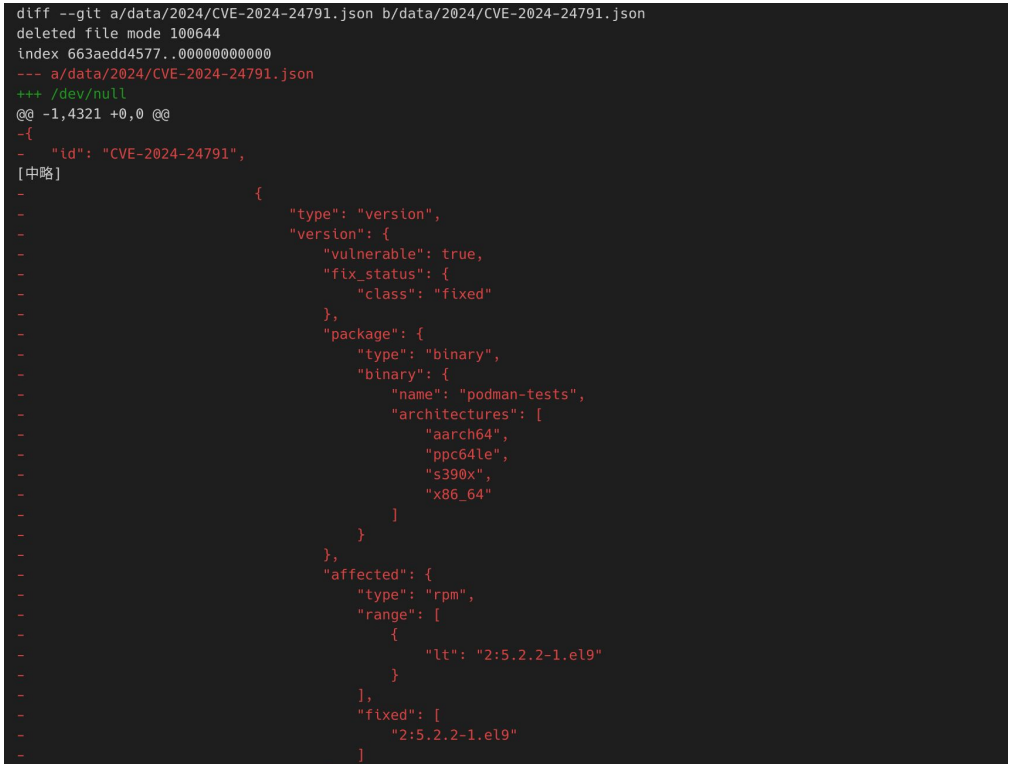
Appendix C.
評価(3): 差分の説明性

OS パッケージに対するステータスの変化

```
diff --git a/data/2024/CVE-2024-0229.json b/data/2024/CVE-2024-0229.json
index ff2d7030545..3ffe8f531ed 100644
--- a/data/2024/CVE-2024-0229.json
+++ b/data/2024/CVE-2024-0229.json
@@ -199,25 +199,41 @@
                                        }
                                ],
                                "published": "2024-01-16T00:00:00Z",
-                               "modified": "2025-01-07T00:57:25Z"
+                               "modified": "2025-07-09T08:20:13Z"
                        },
[中略]
                                                                "version": {
@@ -307,7 +307,7 @@
                                                                        "vulnerable": true,
                                                                        "fix_status": {
                                                                                "class": "unfixed",
-                                                                               "vendor": "Out of support scope"
+                                                                               "vendor": "Affected"
                                                                        },
                                                                        "package": {
                                                                                "type": "source",
@@ -316,7 +316,15 @@
[後略]
```

https://github.com/vulsio/css2025-vuls2#論文-3411-os-パッケージに対するステータスの変化で言及した-cve-2024-0229-の情報

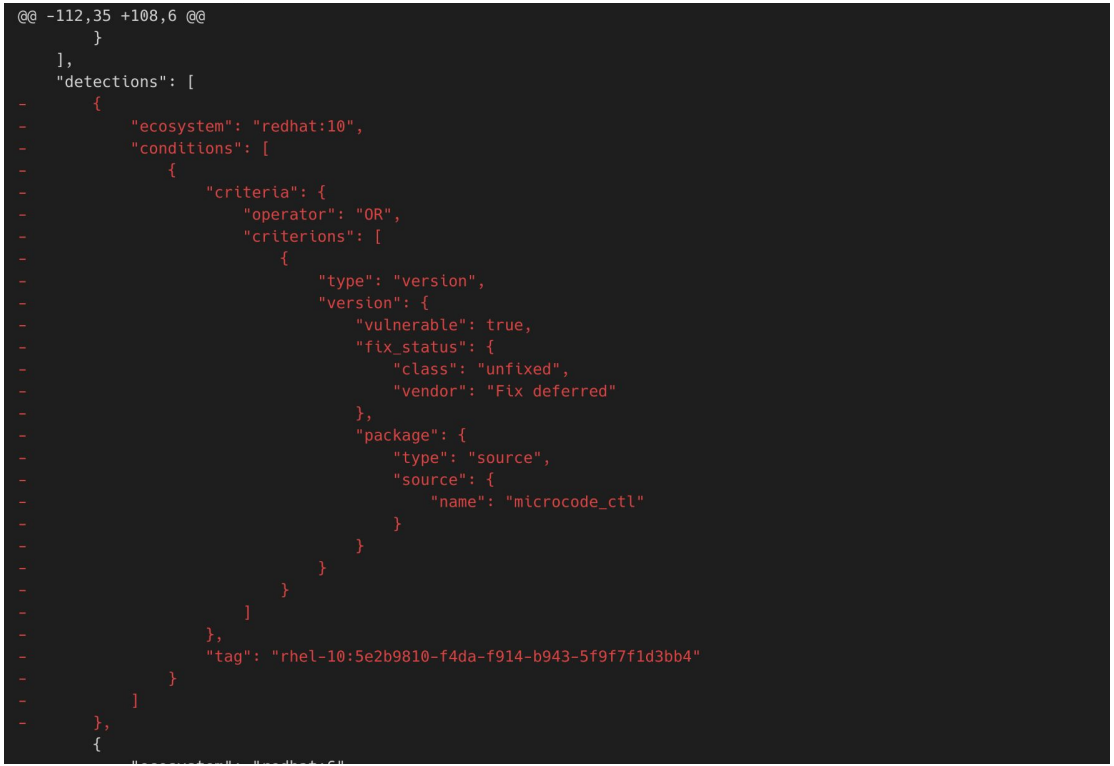
特定の CVE ID に対する情報が消滅する事例



```
diff --git a/data/2024/CVE-2024-24791.json b/data/2024/CVE-2024-24791.json
deleted file mode 100644
index 663aedd4577..00000000000
--- a/data/2024/CVE-2024-24791.json
+++ /dev/null
@@ -1,4321 +0,0 @@
-{
-   "id": "CVE-2024-24791",
[中略]
-                        {
-                            "type": "version",
-                            "version": {
-                                "vulnerable": true,
-                                "fix_status": {
-                                    "class": "fixed"
-                                },
-                                "package": {
-                                    "type": "binary",
-                                    "binary": {
-                                        "name": "podman-tests",
-                                        "architectures": [
-                                            "aarch64",
-                                            "ppc64le",
-                                            "s390x",
-                                            "x86_64"
-                                        ]
-                                    }
-                                },
-                                "affected": {
-                                    "type": "rpm",
-                                    "range": [
-                                        {
-                                            "lt": "2:5.2.2-1.el9"
-                                        }
-                                    ],
-                                    "fixed": [
-                                        "2:5.2.2-1.el9"
-                                    ]
```

https://github.com/vulsio/css2025-vuls2#論文3412-特定の-cve-id-に対する情報が消滅する事例で言及した-cve-2024-24791-の情報

Red Hat 10 に対する情報のみが消滅する事例



```
@@ -112,35 +108,6 @@
         }
     ],
     "detections": [
-        {
-            "ecosystem": "redhat:10",
-            "conditions": [
-                {
-                    "criteria": {
-                        "operator": "OR",
-                        "criterions": [
-                            {
-                                "type": "version",
-                                "version": {
-                                    "vulnerable": true,
-                                    "fix_status": {
-                                        "class": "unfixed",
-                                        "vendor": "Fix deferred"
-                                    },
-                                    "package": {
-                                        "type": "source",
-                                        "source": {
-                                            "name": "microcode_ctl"
-                                        }
-                                    }
-                                }
-                            }
-                        ]
-                    },
-                    "tag": "rhel-10:5e2b9810-f4da-f914-b943-5f9f7f1d3bb4"
-                }
-            ]
-        },
         {
```

https://github.com/vulsio/css2025-vuls2#論文3413-red-hat-10-に対する情報のみが消滅する事例で言及した-cve-2024-43420-の情報