State of the Common Vulnerabilities and Exposures (CVE) Program

November 15, 2023 Workshop

Welcome

- **Today's workshop is oriented towards keeping program stakeholders abreast of key events and details related to:**
  - The state of the CVE Program
  - CVE Services and Authorized Data Publishers (ADPs)
  - Experience with JSON 5.0 and related guidance
  - CVE Program Rules
  - Corpus Hygiene (e.g., link rot, bulk updates)

Questions and comments are welcome! Please use the raise your hand feature in Teams or post your question in the Teams chat window.

CVE Program Mission, Goals, and Desired Outcome

Mission

Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities

Goals

1. Increase CVE Program adoption
   — Increase CVE usage in the vulnerability management ecosystem
2. Increase CVE Program coverage
   — More vulnerabilities get CVE IDs and associated CVE Records

Desired Outcome

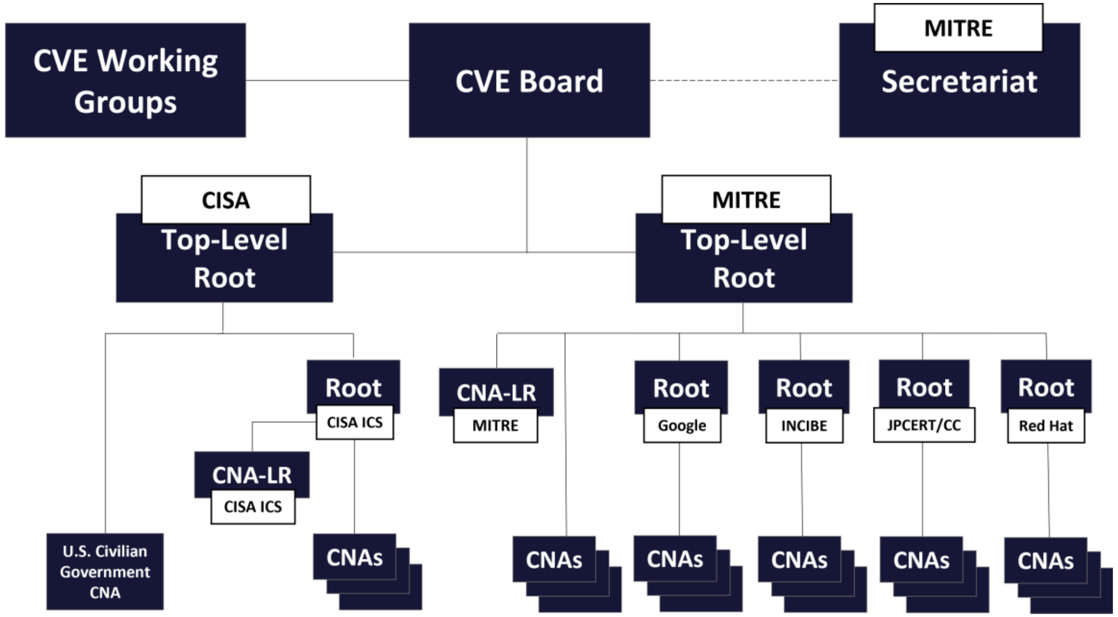
More quality CVE Records are produced, faster

2016-2017: Shift to a Strategy of Federation: Whole of World Partnerships

- **Reinvigorate the CVE Board**
  - Comprised of industry, government, and academic stakeholders
  - Responsible for the strategic direction of the CVE Program
  - Used to meet annually; now meets every two weeks
- **Chart the pathway forward**
  - Develop strategies to scale the program to meet mission outcomes
    - More CNAs and Roots
    - Authorized Data Publishers
    - Working Groups
    - Automated services
    - JSON 5.0
- **Execute and adjust**
  - Keep doing what works, stop doing what does not

Scaling Through Federation: Current Program Structure

- **CVE Board**: The organization responsible for the strategic direction, governance, operational structure, policies, and rules of the CVE Program.
- **CNA**: An organization responsible for the regular assignment of CVE IDs to vulnerabilities, and for creating and publishing information about the vulnerability in the associated CVE Record. Each CNA has a specific Scope of responsibility for vulnerability identification and publishing.
- **Root**: An organization authorized within the CVE Program that is responsible, within a specific Scope, for the recruitment, training, and governance of one or more entities that are a CNA, CNA of Last Resort (CNA-LR), or another Root.
- **Top-Level Root**: A Root that does not report to another Root, and is thus responsible to the CVE Board.
- **CVE Working Group**: An organization created and administered by the CVE Board to accomplish specific objectives through collaboration with CVE stakeholders and the general public where appropriate. Each working group is required to have a charter which defines its area of responsibility, membership, and objectives.

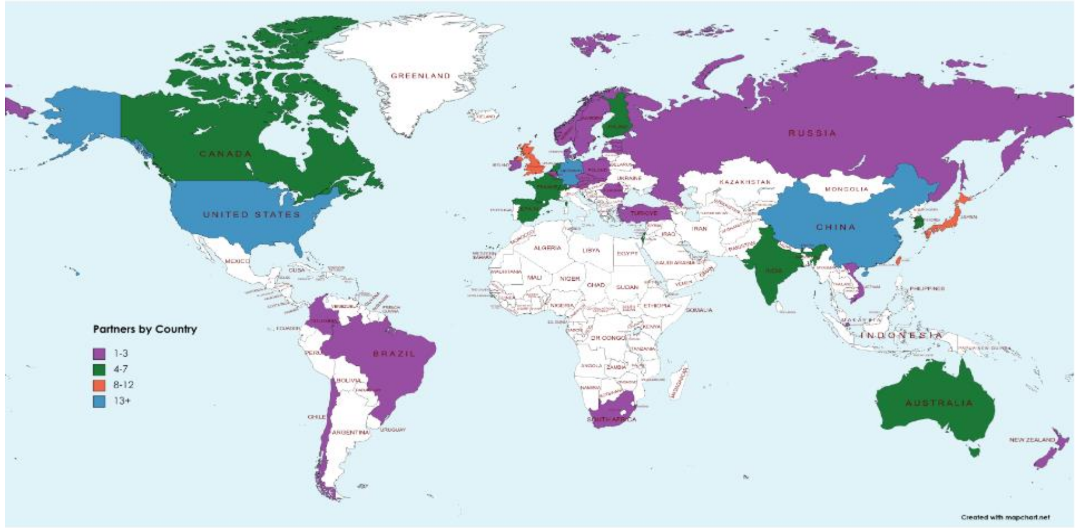


Metrics

	Mission, Goals, Desired Outcome	Value-Based Partnerships		
Calendar Year	Records Published	Number of CNAs	% of Total Production: Volunteer CNAs	% of Total Production: CNA-LRs
2016	6,457	24 (1 Int.)	0%	100%
2017	14,645	78	50%	50%
2018	16,512	90	53%	47%
2019	17,308	106	53%	47%
2020	18,375	144	58%	42%
2021	20,161	209 (100 Int.)	65%	35%
2022	25,059	263 (123 Int.)	68%	32%
2023 (YTD)	22,980	330 (154 Int.)	77%	23%

Federation begins

330 Partners in 37 countries



- **Modernization Metrics**
  - **Four automated services deployed: ID request (IDR), Record Submission and Upload (RSUS), JSON 5.0, CVE.ORG**
  - **CNA onboarding time reduced to two hours from many days**
  - **Program rules, policies, and guidance established and evolving**

Automated Services

- **CVE Services: A client/server architected web application that provides a series of APIs to CNAs that allows them to reserve CVE IDs, submit, update, and publish CVE Records and manage their CVE Services user pool**
  - **CVE ID Reservation (IDR)**: Self-service allowing CNAs to get either an arbitrary number of non-sequential IDs or sequential IDs
    - Status: Deployed December 2020
  - **Record Submission and Upload Subservice (RSUS): Self service allowing CNAs to submit/upload CVE information directly into the CVE Repository, without the need for manual review**
    - Status: Deployed October 2022
  - **CVE User Registry: CVE Program User Provisioning and User management functions that will enable single sign on/single point for service and distributed CVE Service Pool management**
    - Requirements identification and definition underway

CVE Program JSON 5.0 Data Format

- **JSON 5.0 official format and bulk download capability**
  - Hard Deployed March 2023
- **Lessons learned to be discussed in the workshop today**
- **JSON 5.1 (minor release)**
  - Highlight: Supports CVSS 4.0
  - Expected deployment: Q1 CY 2024

Authorized Data Publishers (ADP)

- **An organization authorized by the CVE Program to provide value-added information to CVE Records**
  - Initial pilots underway
    - References
      - Secretariat
    - SSVC: The Stakeholder-specific Vulnerability Categorization (SSVC) is a system for prioritizing actions during vulnerability management
    - KEV: Known Exploited Vulnerabilities
      - CISA
  - Q1 CY24: Move to production
- **Apply to become an ADP through the Strategic Planning Working Group (SPWG)**

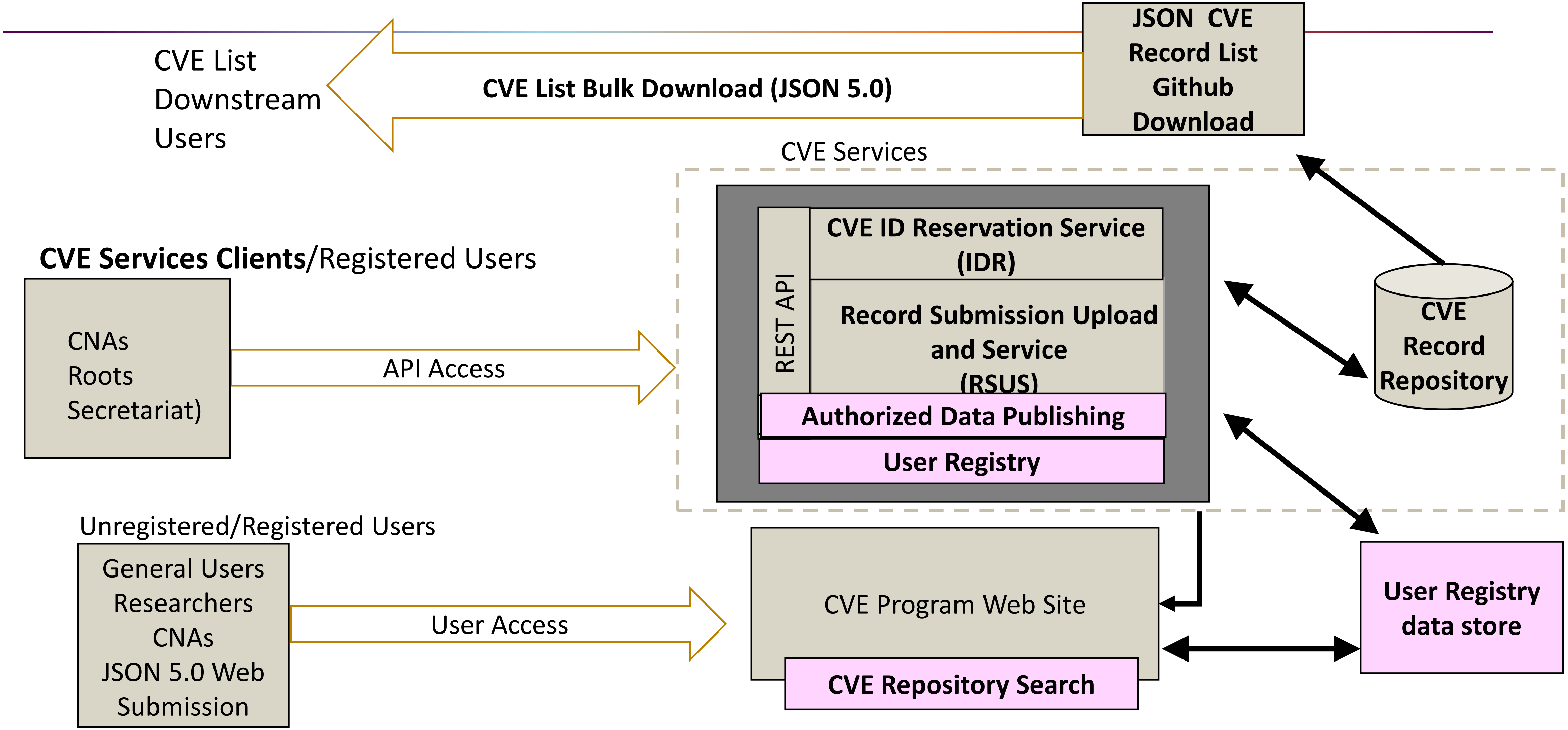
Working Groups

- **Automation (Open to the public)**
  - Focused on identifying and advancing proposals for the collaborative design, development, and deployment of automated capabilities that support the efficient management of the CVE Program.
- **Strategic Planning (Invitation only)**
  - Focused on the long-term strategy (1-5 years) and goals of the CVE Program; works closely with the CVE Board to determine goals and objectives and will act to achieve them.
- **Outreach and Communications (Open to the public)**
  - Promotes the CVE Program to achieve program adoption and coverage goals through increased community awareness.
- **CNA Coordination (Must be a CNA)**
  - Provides a forum for more effective communication and participation by the CNAs.
- **Quality (Open to the public)**
  - Focused on identifying areas where CVE content, rules, guidelines, and best practices must improve to better support stakeholder use cases.

CVE Program Automation Status

CVE Program Workshop, November 15, 2023

CVE Program Automation Target Architecture



JSON CVE Record List Github Download

CVE List Bulk Download (JSON 5.0)

CVE List Downstream Users

CVE Services

CVE ID Reservation Service (IDR)

REST API

Record Submission Upload and Service (RSUS)

Authorized Data Publishing

User Registry

CVE Record Repository

CVE Services Clients/Registered Users

CNAs
Roots
Secretariat)

API Access

Unregistered/Registered Users

General Users
Researchers
CNAs
JSON 5.0 Web Submission

User Access

CVE Program Web Site

CVE Repository Search

User Registry data store

CVE Services

- **A Web Application that provides functions to allow CNAs to:**
  - Reserve CVE IDs,
  - Publish/Update CVE Records
  - Reject CVE IDs/CVE Record
  - Manage their own CVE Services User Pool
- **Function implemented through an API that is accessed by CVE Services Clients**

CVE Services (cont)

To Use CVE Services, CNAs must ….

- **Obtain a CVE Services Account on the appropriate system**
  - – CVE Services PRODUCTION System
  - – CVE Services Test System

https://www.cve.org/AllResources/CveServices#obtaining-credentials

CVE is sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022, The MITRE Corporation. CVE is a registered trademark and the CVE logo is a trademark of The MITRE Corporation.

CNAs must (cont) …

- **Use an available CVE Service client**
  - Vulnogram (GUI)
  - cveClient (GUI)
  - Cvelib (CLI)

OR

- **Create your own CVE Services Client using the CVE Service API**
  - Production API Documntation: https://cveawg.mitre.org/api-docs/

https://www.cve.org/AllResources/CveServices#using-cve-services-clients

CVE is sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2021, The MITRE Corporation. CVE is a registered trademark and the CVE logo is a trademark of The MITRE Corporation.

CVE Services (cont)

CVE Services Guidance Videos

https://www.cve.org/AllResources/CveServices

CVE Program Web Site

- **https://www.cve.org or https://cve.org**
  - Currently in Phased Deployments
  - Contains all CVE Program information and allows for CVE Record Lookup
- **https://cve.mitre.org** still exists as we continue to migrate functions and data
  - Targeted deprecation date: June 2024

Bulk Download

- **Newest Capability (fielded in March/2023)**
  - Allows downstream users to “bulk” download and maintain their own copy of the CVE List
  - Located at: https://github.com/CVEProject/cvelistV5/tree/main/cves
  - A “read only” github repository
  - updates approximately every 15 minutes

Bulk Download (cont)

- **Downstream Users can use one of four methods to view/obtain/maintain the latest JSON 5.0 CVE Records in the CVE List**

1. Peruse the CVE List Github Repository using a standard web browser (view)

2. “clone” the cvelistV5 repository using git technology (i.e.,) *git clone*) and receive updates using standard *git* commands (e.g, *git pull*)

Bulk Download (cont)

3. Download a full “zipped” copy of the full repository:
   - https://www.cve.org/Download

4. Download zipped, incremental hourly updates from the github “Releases” page
   - https://github.com/CVEProject/cvelistV5#releases

Readme: GitHub - CVEProject/cvelistV5: CVE cache of the official CVE List in CVE JSON 5.0 format

Additional Bulk Download Training material to be available in early 2024.

CVE is sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999-2022, The MITRE Corporation. CVE is a registered trademark and the CVE logo is a trademark of The MITRE Corporation.

Current CVE Program Automation Priorities

Authorized Data Publisher (ADP) Capability

- **Capability Need:**
  - Allow enhancement of CVE Records with additional data provided by “authorized” organizations/individuals

- **Status:**
  - Prototype technology currently being piloted
    - New interfaces for CVE Services
  - 2 pilot “Authorized Data Publishers” being considered by the CVE Program
    - Reference Additions (Secretariat)
    - SSVC, KEV Information (CISA)
  - ADP policy/guidance being developed by the SPWG

For those interested in becoming an ADP, contact the SPWG for the ADP Application

CVE Repository Search Capability (Web Site)

- **Capability Need:**
  - Allow Users to perform a robust search of the CVE List from the CVE Program Web Site (i.e., cve.org)
    - Replace search capability currently available on https://cve.mitre.org

- **Status:**
  - Prototype technology completed against Initial Operating Capability (IOC) requirements approved by the Tactical Working Group
  - Targeted for release for testing/community review by the end CY/2023

User Registry

- **Capability Need:**
  - A database to store/manage information that is required to operate the CVE Program to include working user information/authorizations, CNA organizational membership and Working Group information.

- **Status:**
  - Requirements generation underway
  - Development expected to begin in early 2024

Important upcoming events

- **CVE Record Format JSON 4.0 Deprecation**
  - Reduced support for JSON 4.0 download formats to begin in January/2024.
  - Full JSON 4.0 format deprecation scheduled for June 30, 2024
    - https://www.cve.org/Media/News/item/blog/2023/07/25/Legacy-Downloads-being-Phased-Out
- **CVE Services Technical Workshop**
  - 1st QT 2024, date TBD (look for announcement/invitations)
  - In depth look at the CVE Program Automation (and what you need to do to effectively use it)

CVE is sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022 The MITRE Corporation. CVE is a registered trademark and the CVE logo is a trademark of The MITRE Corporation.

Get involved !!

Have questions/ideas on how best to develop and operate the CVE Automation Infrastructure?

Join the CVE Program Automation Working Group (AWG)

- Open Group, all welcome
- Meets every Tuesday from 4:00 – 5:00 PM Eastern Time (Microsoft Teams Meeting)
- Contact the AWG Chair for invite: rbritton@mitre.org

CVE JSON Record Format

Version 5.1 overview

What does a CVE Record contain?

CVE-2020-0001

DL I1234568

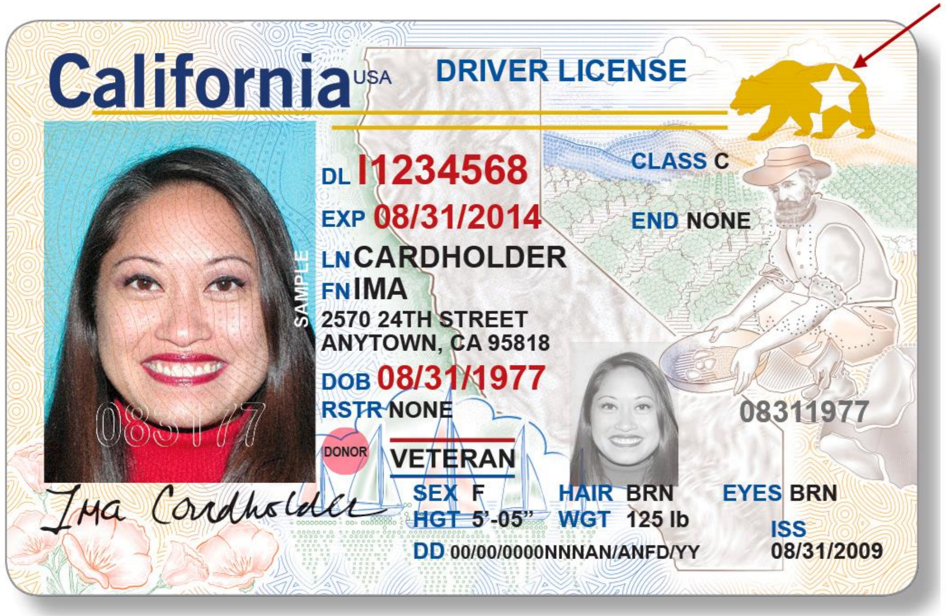
The ID by itself does not contain much information

CVE Record provides context to a CVE ID

CVE-2020-0001

DL **I1234568**

In getProcessRecordLocked of ActivityManagerService.java isolated apps are not handled correctly. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-8.0, Android-8.1, Android-9, and Android-10 Android ID: A-140055304



Minimum information in a record

ID

CNA

affected things

public reference

Additionally useful information

dates

credits

scores

translations

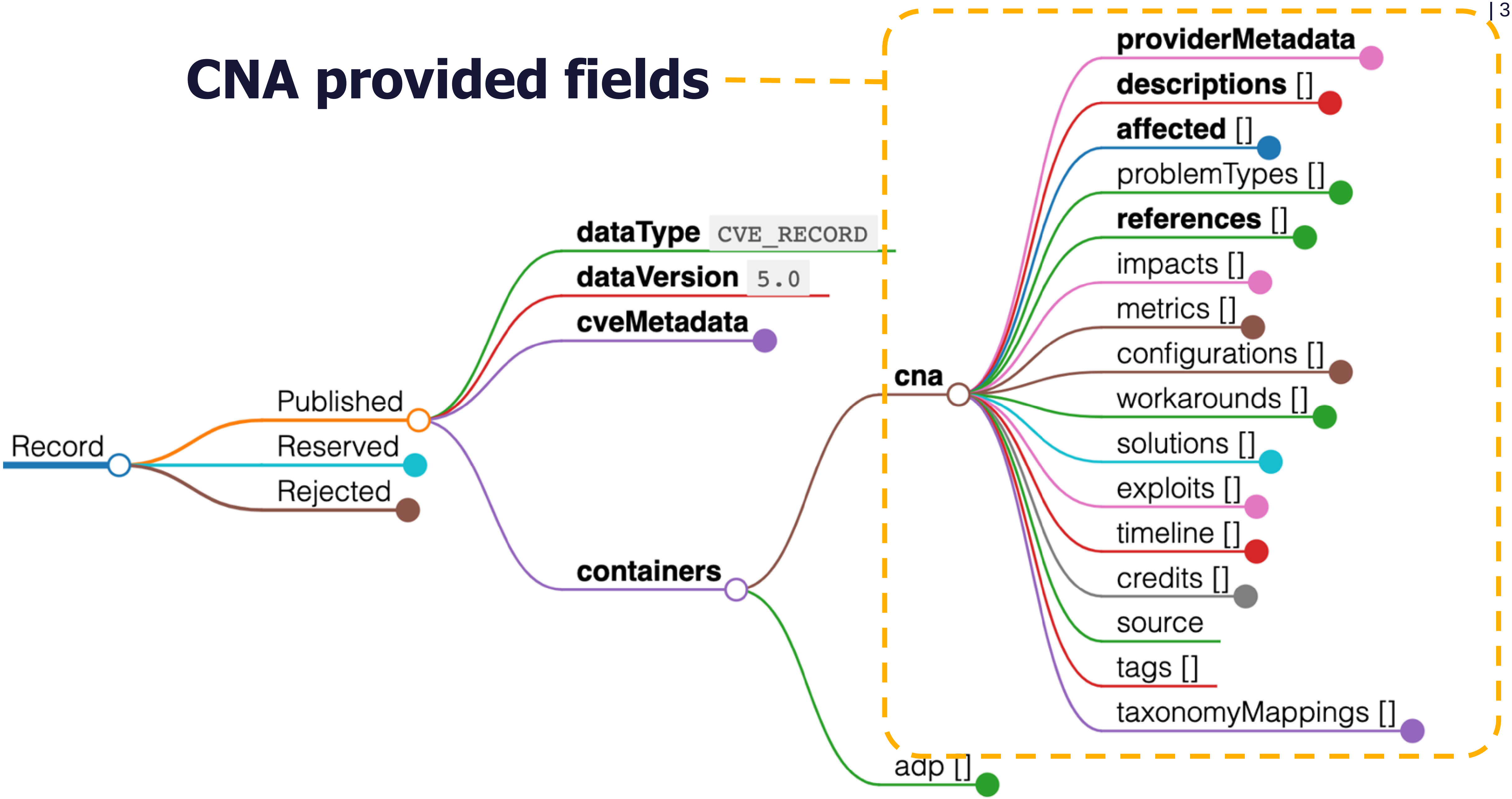
type of vulnerability

solutions

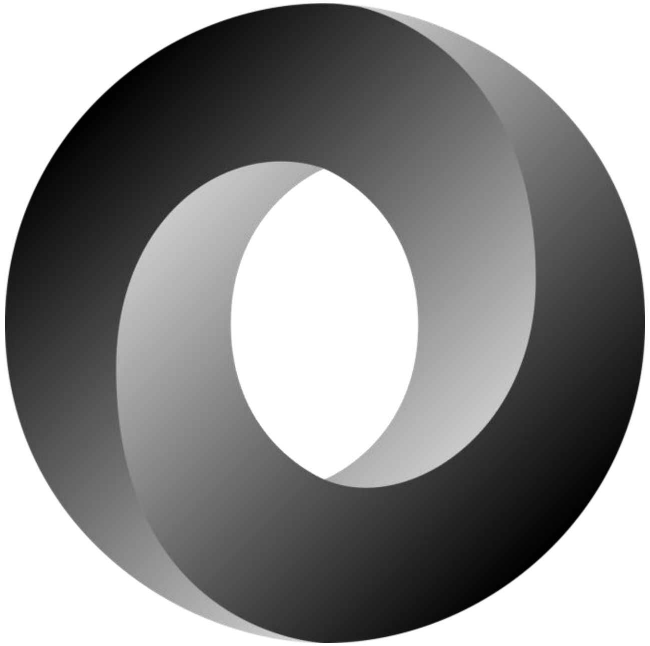
impact

exploits

CNA provided fields



Why JSON?



JavaScript Object Notation (JSON) is a lightweight data-interchange format.

Easy for humans to understand, organize.

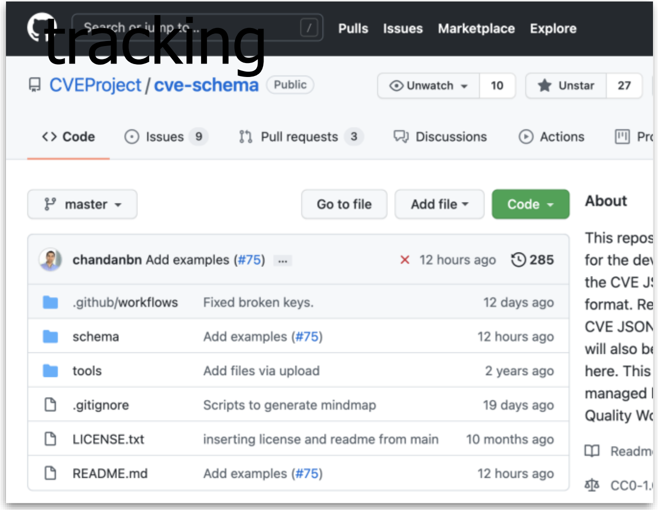
It is easy for machines to encode, parse, validate, and use.

A JSON Schema to codify rules:

- **data types (strings, numbers, dates, arrays)**
- **required fields**
- **valid values and patterns (minimum, maximum, regex)**

Resources

Git repo, issue tracking



Search or jump to... / Pulls Issues Marketplace Explore

CVEProject / cve-schema Public

Unwatch 10 | Unstar 27

Code | Issues 9 | Pull requests 3 | Discussions | Actions | Pro

master | Go to file | Add file | Code

chandanbn Add examples (#75) ... ✕ 12 hours ago 285

.github/workflows	Fixed broken keys.	12 days ago
schema	Add examples (#75)	12 hours ago
tools	Add files via upload	2 years ago
.gitignore	Scripts to generate mindmap	19 days ago
LICENSE.txt	inserting license and readme from main	10 months ago
README.md	Add examples (#75)	12 hours ago

About

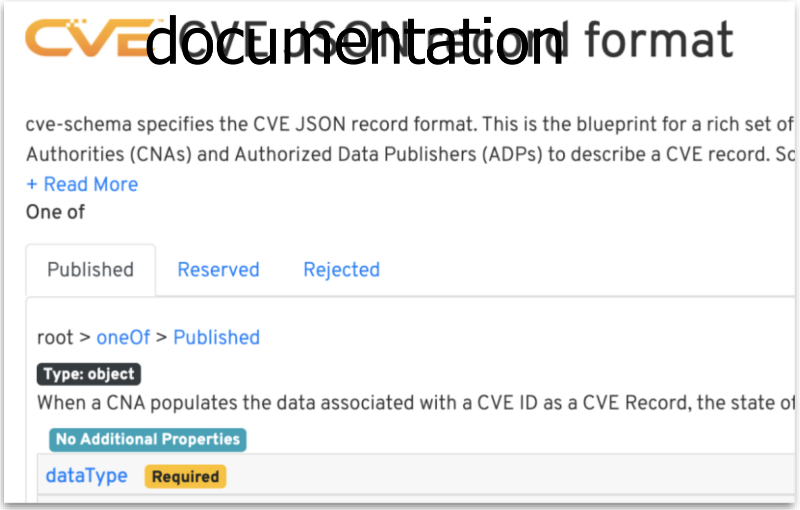
This repos for the dev the CVE JS format. Re CVE JSON will also be here. This managed I Quality Wo

Readm

CC0-1.

github.com/CVEProject/cve-schema

Online documentation



CVE JSON record format

cve-schema specifies the CVE JSON record format. This is the blueprint for a rich set of Authorities (CNAs) and Authorized Data Publishers (ADPs) to describe a CVE record. Sc

+ Read More

One of

Published | Reserved | Rejected

root > oneOf > Published

Type: object

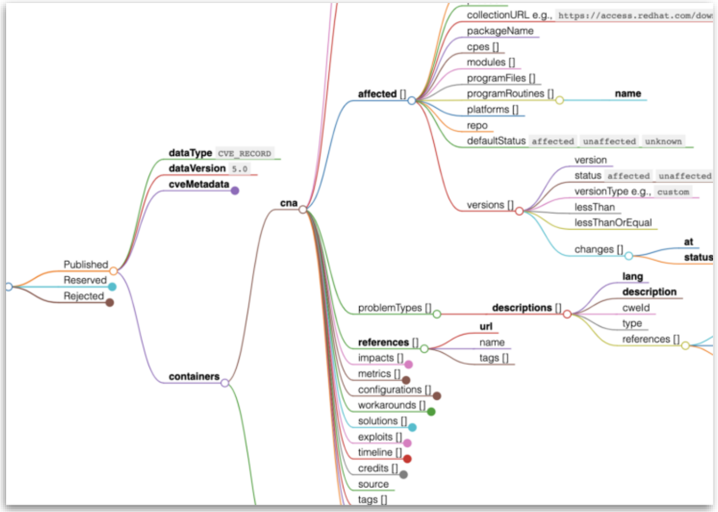
When a CNA populates the data associated with a CVE ID as a CVE Record, the state of

No Additional Properties

dataType Required

cveproject.github.io/cve-schema/schema/v5.0/docs/

Mindmap



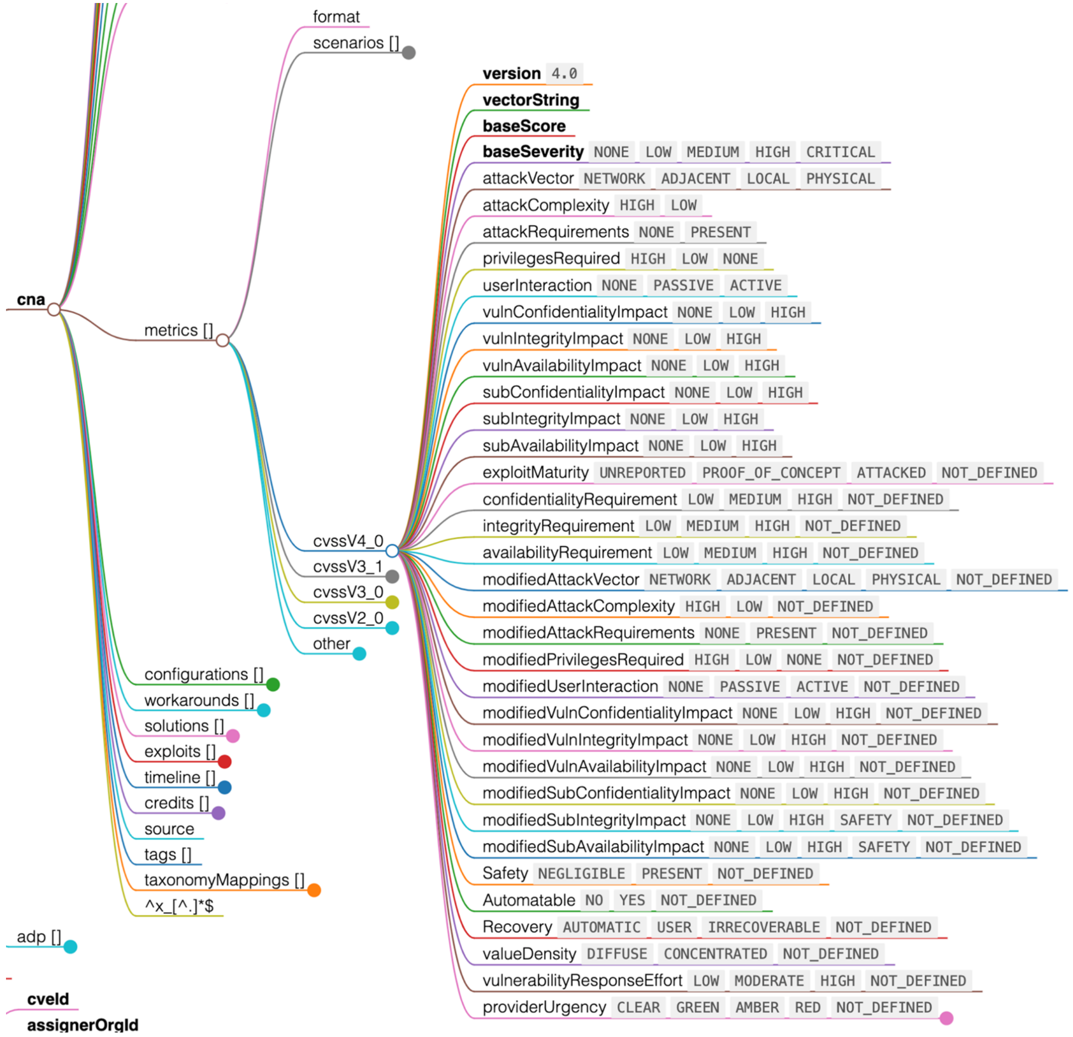
cveproject.github.io/cve-schema/schema/v5.0/docs/mindmap

Copyright © 1999–2023, The MITRE Corporation. CVE and the CVE logo are registered trademarks of The MITRE Corporation.

Changes in CVE JSON 5.1

Support for CVSS v4.0 objects

In addition to a numerical score and a qualitative severity rating, a CVSS 4.0 provides several new attributes related to the vulnerability that include urgency, safety impact, and effort required to respond to the vulnerability.



cna
metrics []
format
scenarios []
cvssV4_0
cvssV3_1
cvssV3_0
cvssV2_0
other
configurations []
workarounds []
solutions []
exploits []
timeline []
credits []
source
tags []
taxonomyMappings []
^x_[^.]*$
adp []
cveId
assignerOrgId

version 4.0
vectorString
baseScore
baseSeverity NONE LOW MEDIUM HIGH CRITICAL
attackVector NETWORK ADJACENT LOCAL PHYSICAL
attackComplexity HIGH LOW
attackRequirements NONE PRESENT
privilegesRequired HIGH LOW NONE
userInteraction NONE PASSIVE ACTIVE
vulnConfidentialityImpact NONE LOW HIGH
vulnIntegrityImpact NONE LOW HIGH
vulnAvailabilityImpact NONE LOW HIGH
subConfidentialityImpact NONE LOW HIGH
subIntegrityImpact NONE LOW HIGH
subAvailabilityImpact NONE LOW HIGH
exploitMaturity UNREPORTED PROOF_OF_CONCEPT ATTACKED NOT_DEFINED
confidentialityRequirement LOW MEDIUM HIGH NOT_DEFINED
integrityRequirement LOW MEDIUM HIGH NOT_DEFINED
availabilityRequirement LOW MEDIUM HIGH NOT_DEFINED
modifiedAttackVector NETWORK ADJACENT LOCAL PHYSICAL NOT_DEFINED
modifiedAttackComplexity HIGH LOW NOT_DEFINED
modifiedAttackRequirements NONE PRESENT NOT_DEFINED
modifiedPrivilegesRequired HIGH LOW NONE NOT_DEFINED
modifiedUserInteraction NONE PASSIVE ACTIVE NOT_DEFINED
modifiedVulnConfidentialityImpact NONE LOW HIGH NOT_DEFINED
modifiedVulnIntegrityImpact NONE LOW HIGH NOT_DEFINED
modifiedVulnAvailabilityImpact NONE LOW HIGH NOT_DEFINED
modifiedSubConfidentialityImpact NONE LOW HIGH NOT_DEFINED
modifiedSubIntegrityImpact NONE LOW HIGH SAFETY NOT_DEFINED
modifiedSubAvailabilityImpact NONE LOW HIGH SAFETY NOT_DEFINED
Safety NEGLIGIBLE PRESENT NOT_DEFINED
Automatable NO YES NOT_DEFINED
Recovery AUTOMATIC USER IRRECOVERABLE NOT_DEFINED
valueDensity DIFFUSE CONCENTRATED NOT_DEFINED
vulnerabilityResponseEffort LOW MODERATE HIGH NOT_DEFINED
providerUrgency CLEAR GREEN AMBER RED NOT_DEFINED

Prevent typos, copy paste mistakes

- **This ensures typos in field names or misplaced fields in CVE record are identified prior to a record's acceptance by the services.**
- **Prevents unexpected fields in the CVE Record.**
- **Hand editing or copy pasting JSON may introduce unintended mistakes.**

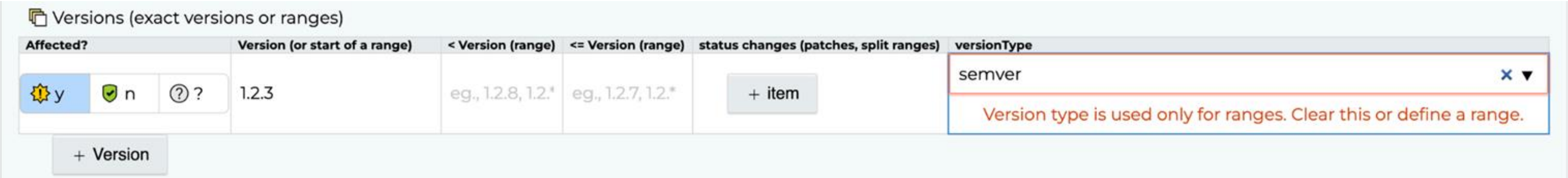
“`None`”: “.....”

“`refsource`” field inside reference object.

`cweID, cweid, or CWE-ID` instead of `cweId`

versionType is now allowed for single version values

With 5.0:

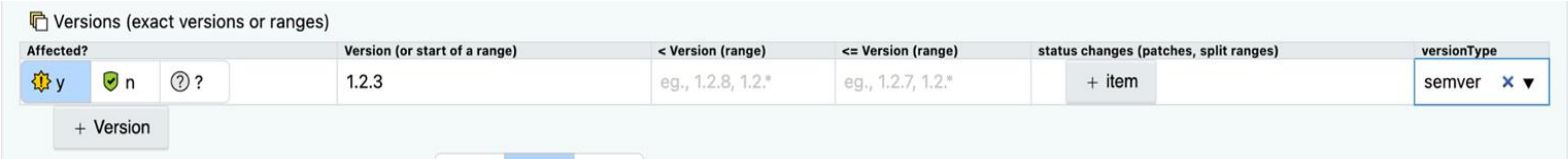


Versions (exact versions or ranges)

Affected?	Version (or start of a range)	< Version (range)	<= Version (range)	status changes (patches, split ranges)	versionType
y n ?	1.2.3	eg., 1.2.8, 1.2.*	eg., 1.2.7, 1.2.*	+ item	semver × ▼ Version type is used only for ranges. Clear this or define a range.

+ Version

With 5.1



Versions (exact versions or ranges)

Affected?	Version (or start of a range)	< Version (range)	<= Version (range)	status changes (patches, split ranges)	versionType
y n ?	1.2.3	eg., 1.2.8, 1.2.*	eg., 1.2.7, 1.2.*	+ item	semver × ▼

+ Version

Considerations for CNAs producing JSON records

Valid against 5.0?	Valid against 5.1?	Note
Yes	No (About ~287 records)	Please fix your tooling!
Yes	Yes	You are good!

Considerations for CVE JSON Consumers

Are you validating CVE records retrieved from the CVE services API or cvelistV5 repo against 5.0 schema?

If yes, then please switch to CVE JSON 5.1 when the services transitions to validating against 5.1 schema, followed by a 5.0 if needed (for ~287 records with typos)

There will be failures validating a 5.1 record using 5.0 schema if

- **the record contains CVSS v4 objects**
- **versionType is associated with single version.**

Gotcha’s with CVE-JSON

Quality issues we currently don’t catch

Extra spaces!

```
product: “  Space Explorer”
version: “1.2.3    “
```

Incoherent versions

```
version: “1.2.3”
status: affected

version: “1.2.3”
status: unaffected
```

Incoherent descriptions

“Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt

Score & Severity

```
baseScore: 9.1
baseSeverity: LOW
```

Quality issues we currently don't catch

CVSS vector and scores mismatch!

```
vectorString:
"CVSS:3.1/AV:N/AC:L/PR:
N/UI:N/S:C/C:H/I:H/A:H"
baseScore: 1.0
```

Nothing is vulnerable!

```
version: "1.2.3"
status: unaffected

version: "1.2.4"
status: unaffected

defaultStatus:unaffected
```

Quality issues we currently don’t catch

LinkRot

```
url: www.error404.com
```

Future CVE-JSON Updates

Future CVE-JSON Updates

CVSS Version Tags Hardcoded

`Current: "cvssV3_1": {…`

Future version of schema could move version to a score array

Root Cause CVE Level Tags

Include a tag in the CNA or ADP container that identifies whether a CVE has hardware or software root cause

CNA and ADP data removed in a REJECTED record

Would be useful to persist this legacy data to allow consumers to still access the previously posted data

productId of type "uuidType" in the "product" object

Lots of CNAs who could add product uuid. Allow consumers of the CVE data allow to easily identify a product, independent of the product name

CNA Operational Rules Update

Kent Landfield
Art Manion
Strategic Planning Working Group (SPWG)

Status

- **Revision started quite some time ago**
  - March 2023
  - Extended meetings since July 2023
- **Almost done**
  - Well, SPWG is almost done
  - More on this later
- **Significant content and editorial changes**
  - Ripple effects on EoL, Dispute Resolution, and Glossary
  - More on this later

(Draft) Schedule

- **SPWG produces 1st draft**
  - January 2024
- **CNA review cycle**
  - 4 weeks
  - SPWG adjudicates comments during this period
- **SPWG produces 2nd draft**
  - 2 weeks
  - SPWG finalizes CNA comments
- **WG review cycle**
  - 2 weeks
  - WG chairs determine if and how to handle comment
  - SPWG adjudicates comments during this period

- **SPWG produces final draft**
  - 1 week
  - SPWG finalizes WG comments
- **CNA and WG final review**
  - 1 week
  - Substantial changes likely will not be accepted
- **Board review cycle**
  - 2 weeks
  - Board vote
  - March 2024

(Draft) Schedule

- **Grace period**
  - 90 days
  - Rules are approved but not strictly enforced
  - CNAs may need time to adapt practices to new rules

(Draft) Comment process

- **Google Docs**
  - Possibly an email address also, will prefer Google Docs
- **Comments with suggested changes will be strongly preferred and prioritized**
  - Complaining is cheap
- **Adjudication**
  - Accept typographical errors, grammar and language improvements, clear and minor content improvements, changes with clear consensus
  - Discuss controversial or major changes with commenter and interested parties, seek consensus
  - Ultimately, SPWG decides, Board votes

Highlights

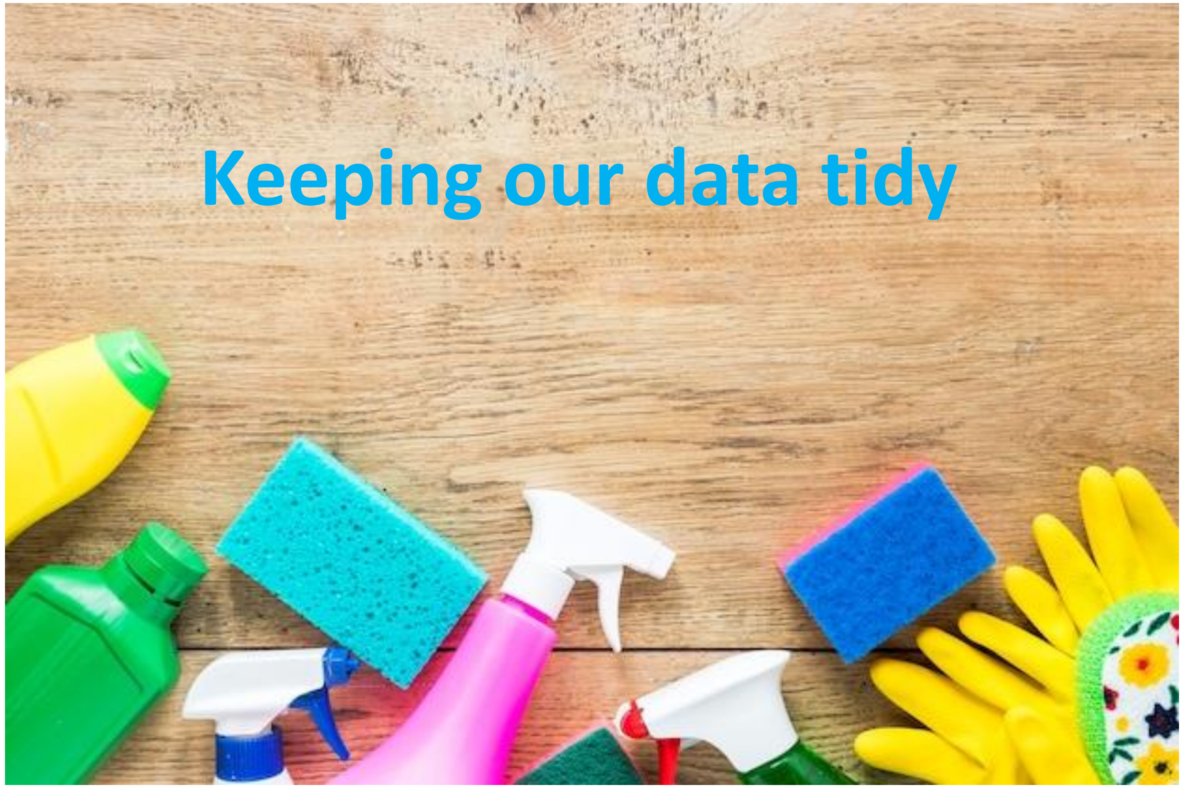
- **Significant rule changes**
  - https://github.com/zmanion/CVE/blob/main/CNA_Rules_changes.md
- **Collecting rule change issues**
  - https://github.com/zmanion/CVE/issues?q=is%3Aissue+is%3Aopen+label%3A%22CNA+rules%22
  - https://github.com/zmanion/CVE/issues?q=is%3Aissue+is%3Aopen+label%3A%22EOL+rules%22

Future updates

- **Program-wide policy documents as markdown in CVE GitHub**
  - Issues, discussions, PRs, releases
  - Transparency, revision control
  - May be transformed for publication on cve.org as HTML or PDF
  - Accommodate non-git/GitHub contributors
- **Regular revision cycle?**
  - Every 6 months?
  - Stagger documents?
  - No changes is OK
  - Out-of-cycle if needed

CVE Corpus Hygiene

Lisa Olson



Tasks for Data Hygiene Maintenance

- Clean up unused CVEs at the end of each year
- Monitor and repair RBPs
- Want to clean up old CVEs?
- JSON lint tools
- Link Rot

RBPs – "Just Publish It!"

Reserved but Public (RBP)	A CVE ID in the "Reserved" state that is referenced in one or more public resources, but for which the details have not be published in a CVE Record.

Total Reserved but Public CVE IDs
------------------------------------ > 5%
Public CVE IDs in the past 12 months

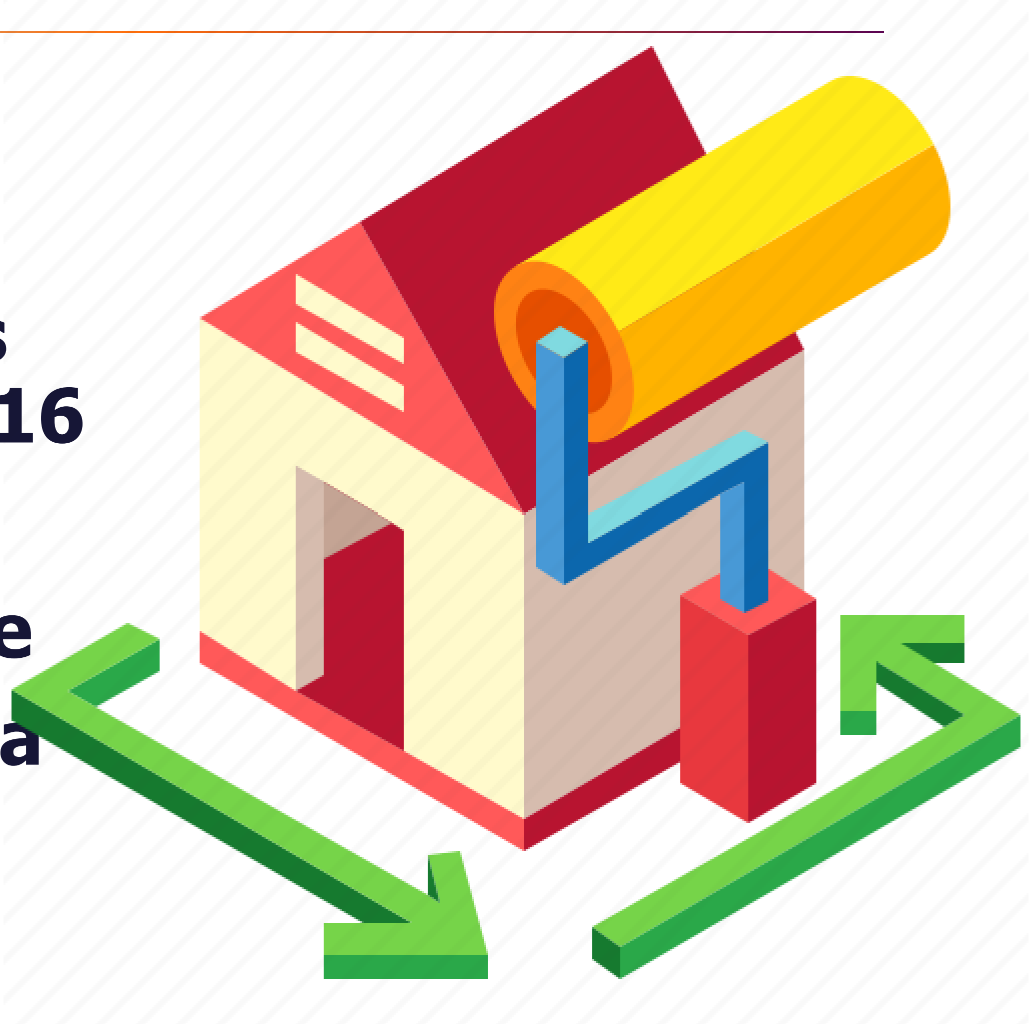
Publish by Nick Youngson CC BY-SA 3.0 Alpha Stock Images

Asked for too many CVEs?

- Different CNA do different things
- If you have extra CVEs at the end of the year and don't want to use them then it is easy to REJECT them.
- There is a way to find out which CVE are reserved

Do you want to update your old CVEs?

- Some of the JSON4 to JSON5 conversion were not perfect
- You can change any of your CVEs in the corpus after October of 2016
- Leave the earlier ones alone
- Don’t try to do all of them at once
- Don’t change the descriptions in a negative way. Improve, don’t obscure



The mission of the CVE Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered then assigned and published by organizations from around the world that have partnered with the CVE Program. Partners publish CVE Records to communicate consistent descriptions of vulnerabilities. Information technology and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities.

Learn more www.cve.org