# CVE Enrichment

## Life without NVD ?

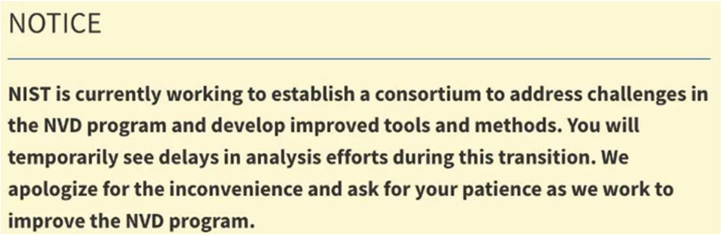
**© *Rob Hulsebos***

Version 20-March-2024

`This article is written on personal title.`

## Introduction

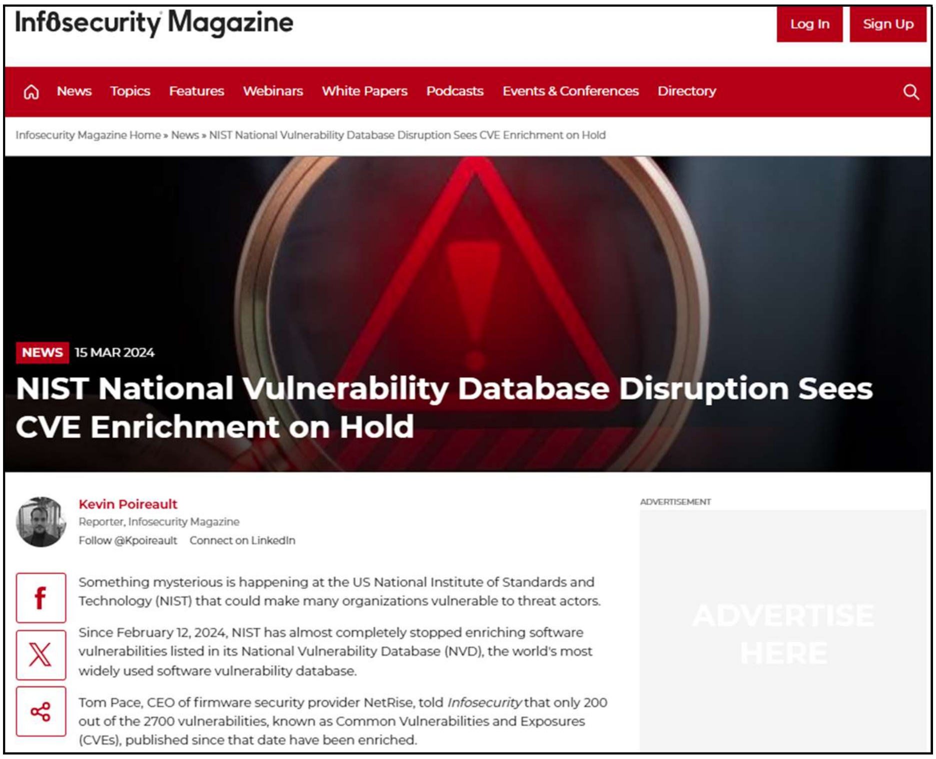
Beginning March 2024, there was some uproar about the NVD (National Vulnerability Database) no longer adding enrichment metadata to CVE's. It started with this announcement in February:



NOTICE

**NIST is currently working to establish a consortium to address challenges in the NVD program and develop improved tools and methods. You will temporarily see delays in analysis efforts during this transition. We apologize for the inconvenience and ask for your patience as we work to improve the NVD program.**

An article in InfoSecurity Magazine[1] nicely describes what is going on:



**NIST National Vulnerability Database Disruption Sees CVE Enrichment on Hold**

Kevin Poireault
Reporter, Infosecurity Magazine
Follow @Kpoireault Connect on LinkedIn

Something mysterious is happening at the US National Institute of Standards and Technology (NIST) that could make many organizations vulnerable to threat actors.

Since February 12, 2024, NIST has almost completely stopped enriching software vulnerabilities listed in its National Vulnerability Database (NVD), the world's most widely used software vulnerability database.

Tom Pace, CEO of firmware security provider NetRise, told *Infosecurity* that only 200 out of the 2700 vulnerabilities, known as Common Vulnerabilities and Exposures (CVEs), published since that date have been enriched.

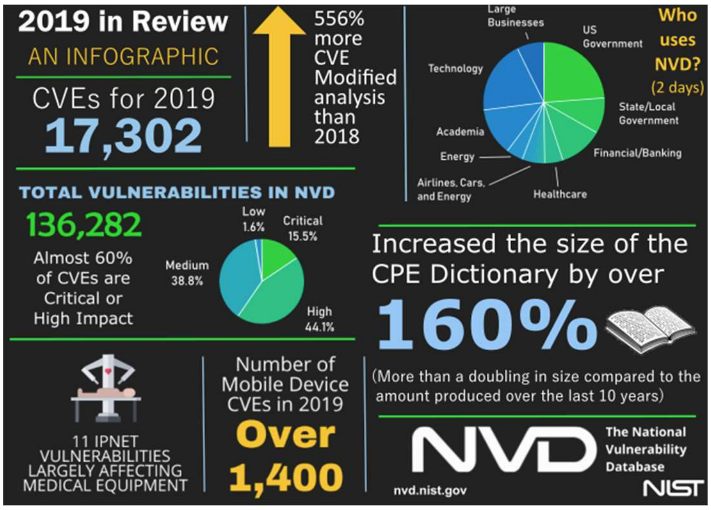
[1] *See https://www.infosecurity-magazine.com/news/nist-vulnerability-database/*

Because the NVD is heavily relied upon as a source of vulnerability information, lacking the enrichment metadata makes it more difficult for automated asset management tools to detect vulnerabilities and inform assets owners.

Other publications, i.e. from ResilientCyber[2] and Anchore[3] addressed the same.

**Reforms**

There have been earlier calls to reform the NVD (see ReversingLabs[4]) but the quite recent (and sudden) issues surprised many.



I don’t envy the NVD in having to process more than 30K CVE’s per year, or about 100 per day on average. Since the number of CVE’s is increasing steadily (i.e. in 2024 twice as much as in 2021) there had to occur a bottleneck somewhere (does the NVD budget grow accordingly? Apparently not – there was a budget cut instead).

**Article**

In the text below, we’ll see what the NVD enrichment entails, and what alternative sources for this enrichment information could be. Spoiler: there is certainly life possible without NVD enrichment, but it isn’t always easy.

**Note**: I’m active in OT cybersecurity, and that perspective on vulnerabilities may be different from what is common in IT cybersecurity.

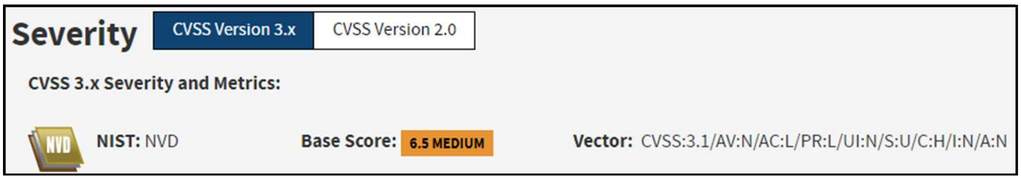
[2] *https://resilientcyber.substack.com/p/death-knell-of-the-nvd*
[3] *https://anchore.com/blog/national-vulnerability-database-opaque-changes-and-unanswered-questions/*
[4] *https://www.reversinglabs.com/blog/gaps-nvd-increases-china-cyber-threat*

# 1 Enrichment - what is it?

Knowing about the existence of a certain vulnerability is not enough to determine what to do: how dangerous is that vulnerability? How can the vulnerability be exploited? Which products/software products are affected? This information can be found in the CVE metadata.

The NVD analyzes the vulnerability and then adds these metadata fields:

- "CVSS" (Common Vulnerability Scoring System), a number in the range 0 – 10 that indicates how dangerous the vulnerability is. The CVSS score is often used to prioritize the handling of the vulnerability, i.e. "CVSS > 7 ? Patch immediately".

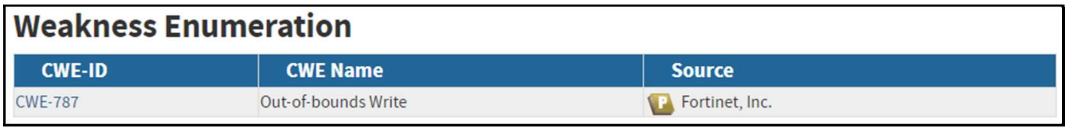


Severity

CVSS 3.x Severity and Metrics:

NIST: NVD    Base Score: 6.5 MEDIUM    Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

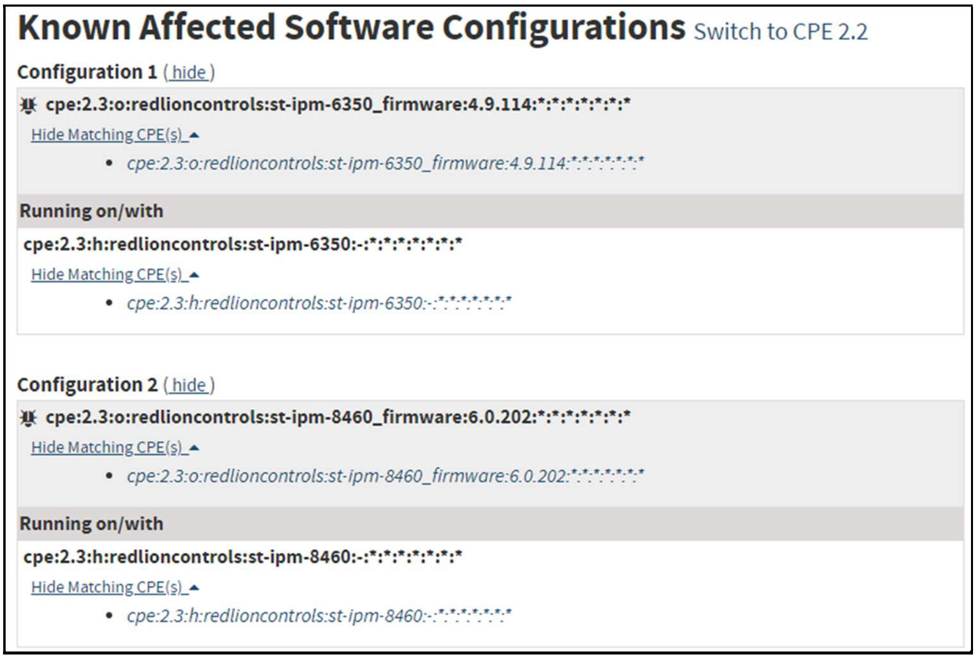
- "CWE" (Common Weakness Enumeration[5]), an entry from the list of software and hardware weaknesses describing the root-cause of the vulnerability.



Weakness Enumeration

| CWE-ID | CWE Name | Source |
|---|---|---|
| CWE-787 | Out-of-bounds Write | Fortinet, Inc. |

- "CPE" (Common Platform Enumeration[6]), describing the know affected software configuration (and/or the hardware platforms it runs on). An example:



Known Affected Software Configurations

Configuration 1 (hide)

cpe:2.3:o:redlioncontrols:st-ipm-6350_firmware:4.9.114:*:*:*:*:*:*:*

- cpe:2.3:o:redlioncontrols:st-ipm-6350_firmware:4.9.114:*:*:*:*:*:*:*

Running on/with

cpe:2.3:h:redlioncontrols:st-ipm-6350:-:*:*:*:*:*:*:*

- cpe:2.3:h:redlioncontrols:st-ipm-6350:-:*:*:*:*:*:*:*

Configuration 2 (hide)

cpe:2.3:o:redlioncontrols:st-ipm-8460_firmware:6.0.202:*:*:*:*:*:*:*

- cpe:2.3:o:redlioncontrols:st-ipm-8460_firmware:6.0.202:*:*:*:*:*:*:*

Running on/with

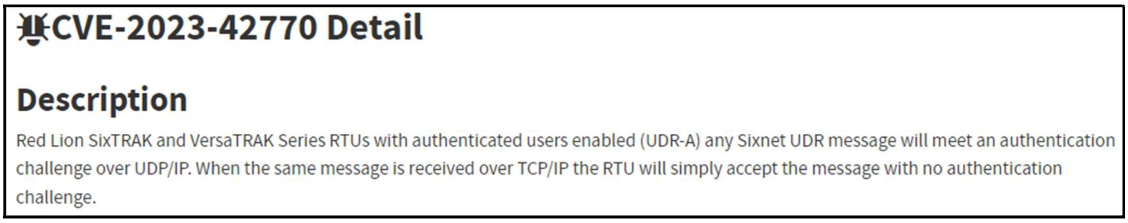
cpe:2.3:h:redlioncontrols:st-ipm-8460:-:*:*:*:*:*:*:*

- cpe:2.3:h:redlioncontrols:st-ipm-8460:-:*:*:*:*:*:*:*

[5] *See https://cwe.mitre.org/data/index.html*
[6] *See https://nvd.nist.gov/products/cpe*

> See the paper from ResilientCyber[7] for more details on CPE's and ongoing discussions on modernizations. However, these developments are not finalized yet and so for the time being we'll have to work with CPE's.

There is also a textual description of the vulnerability, and URL's to other documents (i.e. a vendor advisory, ICSA advisory, researcher publication). Example:



CVE-2023-42770 Detail

Description

Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message is received over TCP/IP the RTU will simply accept the message with no authentication challenge.

**NVD API**

For automated processing of CVE's, the NVD offers an API. The CVE information is provided in JSON format. Accessing the API is free, but there is a limit to the number of requests per minute. However it is sometimes very slow, not responding at all, or drops API requests.

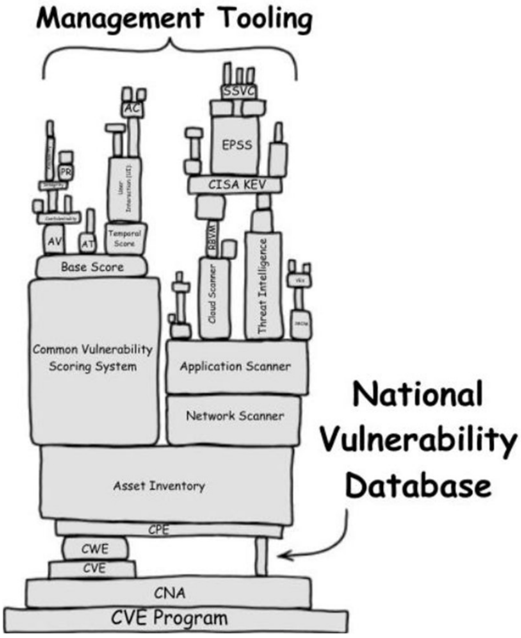
# 2 Enrichment – is it needed?

Quoting from the InfoSecurity-Magazine article, the missing metadata:

> "… leaving organizations blind to what products and systems in their environments the specific vulnerabilities may be impacting."

This is especially true for the CPE's and to a lesser degree for the CVSS.

ResilientCyber in its publication put this picture prophesying doom for any asset management solutions, KEV and EPSS:



[7] https://resilientcyber.substack.com/p/death-knell-of-the-nvd

**Other sources**

Is it really that bad? Is the NVD really the only source for vulnerability data? Are there no other sources? It turns out there are, some other sources of vulnerability information:

- Vendor advisories
- ICSA
- VDE CERT (https://cert.vde.com/en)
- Github Advisory Database (https://github.com/advisories)
- China's NVD[8] (CNVD, https://www.cnnvd.org.cn/)
- Russia's NVD[9] (FSTEC, http://bdu.fstec.ru/vul, Google Translate works very good here)
- Open Source Vulnerability Database (https://osv.dev/)
- …

Useful as they sometimes may be for discovering vulnerabilities outside[10] the CVE database, many refer straight back to the CVE advisories and thus straight back to the NVD. Also, there are usually no CPE's provided, so you may have to work with only the CVSS and/or CWE.

Personally, I found the best source for something that resembles CPE's are: the vendor advisories.

# 3 Enrichment – vendor sources?

Once upon a time the NVD was the *only* source of vulnerability information (and for many it still is) but times have changed. Even ten years ago, many companies hardly published information about vulnerabilities in their products[11].

But times have changed. Many vendors see cybersecurity as important, and they actively inform their customers via their own websites. Almost always[12] these advisories contain CVSS and CWE metadata. There is usually no CPE metadata, but there *are* lists of affected products and/or affected software versions. So, as a customer, you can still proceed to assess whether the vulnerability affects any products you might have from that vendor. The disadvantage is that it cannot be done automatically.

## Example 1

This advisory[13] from Cisco gives all the CVSS / CWE information, only the CPE's are not present (but Cisco lists affected products elsewhere in the advisory):

[8] *Learn more about it at https://www.youtube.com/watch?v=6BtnGo3-K6Y*

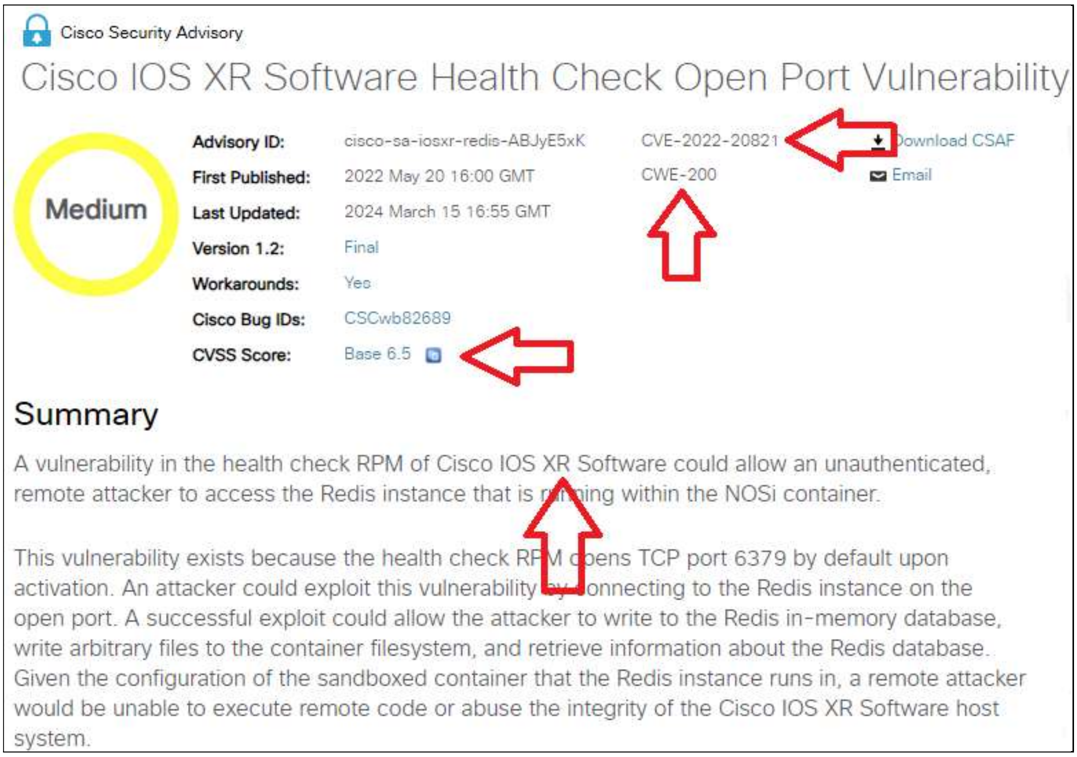
[9] *Learn more about it at https://www.theregister.com/2018/07/17/russia_vuln_database/*

[10] *I once found a vulnerability reported for (Taiwanese) Moxa products reported in FSTEC, but without a CVE.*

[11] *Many companies still don't publish information about vulnerabilities in their products, but that's another issue.*

[12] *Some companies **do** publish advisories, but do not assign a CVE. This makes that it almost doesn't exist in the cybersecurity sphere, i.e. it cannot be added to CISA's "KEV" (Known Exploited Vulnerabilities) list and is also not tracked in the "EPSS" (Exploit Prediction Scoring System). Asset management solutions that solely rely on the NVD cannot track such vulnerabilities.*

[13] *See https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-redis-ABJyE5xK*



Cisco Security Advisory

Cisco IOS XR Software Health Check Open Port Vulnerability

Medium

| | | | |
|---|---|---|---|
| Advisory ID: | cisco-sa-iosxr-redis-ABJyE5xK | CVE-2022-20821 | Download CSAF |
| First Published: | 2022 May 20 16:00 GMT | CWE-200 | Email |
| Last Updated: | 2024 March 15 16:55 GMT | | |
| Version 1.2: | Final | | |
| Workarounds: | Yes | | |
| Cisco Bug IDs: | CSCwb82689 | | |
| CVSS Score: | Base 6.5 | | |

Summary

A vulnerability in the health check RPM of Cisco IOS XR Software could allow an unauthenticated, remote attacker to access the Redis instance that is running within the NOSi container.

This vulnerability exists because the health check RPM opens TCP port 6379 by default upon activation. An attacker could exploit this vulnerability by connecting to the Redis instance on the open port. A successful exploit could allow the attacker to write to the Redis in-memory database, write arbitrary files to the container filesystem, and retrieve information about the Redis database. Given the configuration of the sandboxed container that the Redis instance runs in, a remote attacker would be unable to execute remote code or abuse the integrity of the Cisco IOS XR Software host system.

Additionally, for this vendor, Cisco provides much more details in its advisory then are given in the CVE, so it's wise to make the Cisco website vendor advisory your starting point if you have Cisco in our network.

Also, there is help to automate processing – Cisco publishes a CSAF file (see below) with its advisories. My experience with Cisco CSAF's (and the older format CVRF) is that they contain data about affected software/firmware versions and affected products. You don't need any CPE's!

**Sidenote: What is CSAF?**

CSAF (Common Security Advisory Framework) is a JSON-based description of vulnerability advisories which is now making inroads. Several larger and smaller vendors now started using CSAF[14], i.e. (IT vendors) Cisco, FortiNet and (OT vendors) Siemens and Schneider Electric. It makes the automated processing of vendor advisories possible – this could not be done in the past, there was no common format[15] for automated processing.

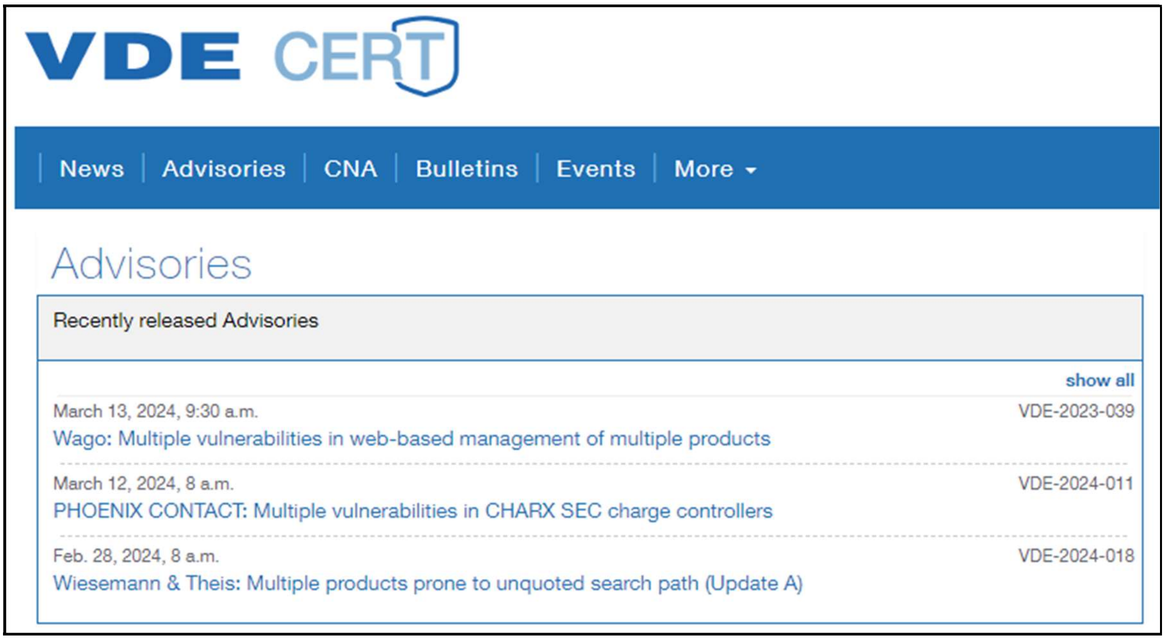
Apart from CSAF, I also see usage of the Vuln-O-Gram file format, i.e. as used by QNAP and Rockwell Automation, but this format is more limited than CSAF. But it is better than nothing.

*[14] A successor of the older CVRF (Common Vulnerability Reporting Format), which was so common that hardly any vendor supported it (notable exceptions: Cisco and FortiGuard Labs).*

*[15] Of course one could process PDF, HTML, TXT and other file formats, but there was no common format between vendors, and how the information was structured in a file.*

# Example 2

As a typical example for the OT community, take the website of the (German) VDE-CERT (https://cert.vde.com/en/advisories/), listing the cybersecurity advisories from some (German) 30+ OT companies.



Advisories

Recently released Advisories

show all

March 13, 2024, 9:30 a.m. VDE-2023-039
Wago: Multiple vulnerabilities in web-based management of multiple products

March 12, 2024, 8 a.m. VDE-2024-011
PHOENIX CONTACT: Multiple vulnerabilities in CHARX SEC charge controllers

Feb. 28, 2024, 8 a.m. VDE-2024-018
Wiesemann & Theis: Multiple products prone to unquoted search path (Update A)

Although the advisories still refer back to the NVD (and the CPE's) it is no solution to get missing CPE's, but it solves your issue in not having to track lots of separate vendor websites.

# Summary

The information being available in vendor advisories is not a 100% solution to the NVD problem, because vendor advisories are ignored by many. But: it doesn't take more than a visit to your favorite vendor's website to find vulnerability information.

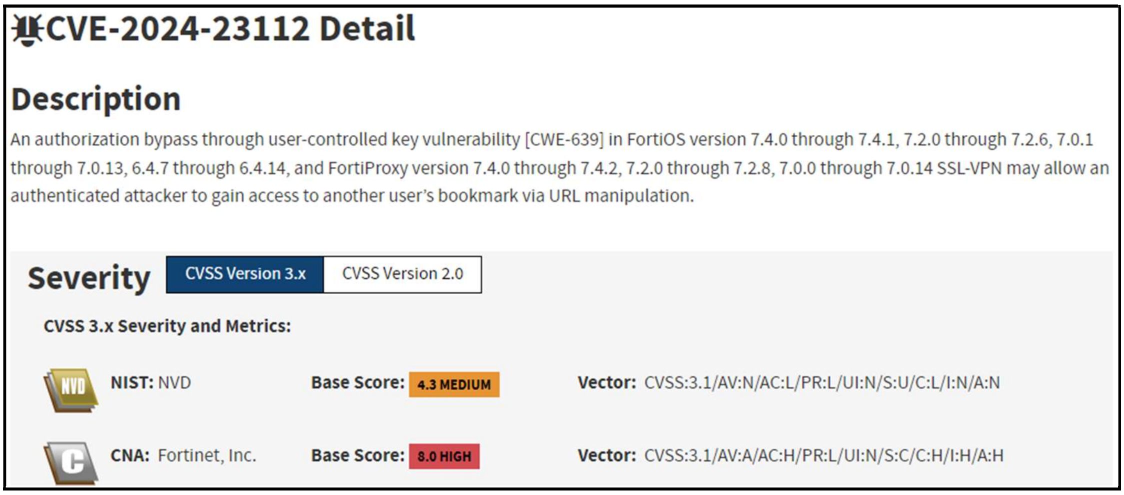
Vendor information about affected products may not be in CPE syntax, but at least it is a (usually) a very recognizable description of the affected hardware /software. If you are a customer of that vendor, you'll very likely recognize the products mentioned.

Using vendor advisories also has the advantage that it is "the source of truth" about vulnerabilities. The advisory is available earlier than on the NVD (and/or ICSA) so you can act quicker. Also I often see copy/paste errors in the NVD information (and/or sometimes also in ICSA, if there is any for an OT product).

# 4 Enrichment – effort duplication

In cases where the NVD has enriched a CVE, it is sometimes seen that there is a duplication of effort. For example, a CVE may have multiple CVSS scores – one from the vendor, and one from the NVD. This wouldn't be a problem if the CVSS scores are identical. But often they are not, and may even vary widely.

This is an issue for product owners, as they often use the CVSS score to decide how to handle the vulnerability: the difference between a "H" (= immediate action) or an "M" (= schedule for later handling) is important.



**CVE-2024-23112 Detail**

**Description**

An authorization bypass through user-controlled key vulnerability [CWE-639] in FortiOS version 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.1 through 7.0.13, 6.4.7 through 6.4.14, and FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14 SSL-VPN may allow an authenticated attacker to gain access to another user's bookmark via URL manipulation.

**CVSS 3.x Severity and Metrics:**

**NIST:** NVD **Base Score:** 4.3 MEDIUM **Vector:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

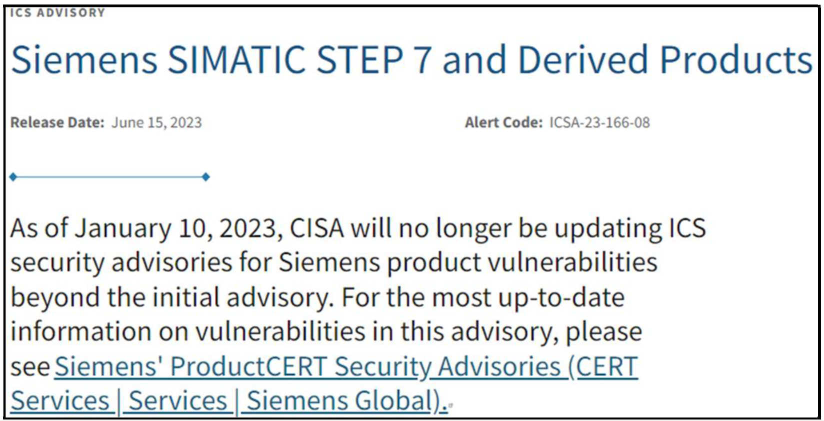
**CNA:** Fortinet, Inc. **Base Score:** 8.0 HIGH **Vector:** CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

*Figure: an example of a recent CVE with widely varying CVSS scores*

Personally, I often wonder where the differences between CVSS scores come from, does the NVD know any better than the vendor? And on which data is this alternative decision based? I'd encourage to put more trust in the vendor's assessment of a vulnerability, prevent double effort, and prevent user confusion.

Another effort duplication I noticed is the usage of CSAF's (Common Security Advisory Framework). CISA now also supports CSAF for all its recent ICSA advisories, which greatly helps to promote CSAF for OT vulnerability reporting. However, one thing I don't understand here is why an advisory may now have two different CSAF's – one from the original vendor and one from CISA itself. If CSAF's are so good for automated handling of vulnerability advisories, why cannot CISA ingest the vendor CSAF? Again duplicate work, with all associated issues.

Also CISA has stopped supporting handling updates from Siemens, making CISA advisory publications for Siemens not reliable (how do you know the ICSA CSAF is still the most up-to-date? Better go to the Siemens website directly and skip CISA completely).



ICS ADVISORY

**Siemens SIMATIC STEP 7 and Derived Products**

**Release Date:** June 15, 2023 **Alert Code:** ICSA-23-166-08

As of January 10, 2023, CISA will no longer be updating ICS security advisories for Siemens product vulnerabilities beyond the initial advisory. For the most up-to-date information on vulnerabilities in this advisory, please see Siemens' ProductCERT Security Advisories (CERT Services | Services | Siemens Global).

# 5 Enrichment - quality

Not only the *presence* of metadata in CVE’s is important, but also the *quality*:

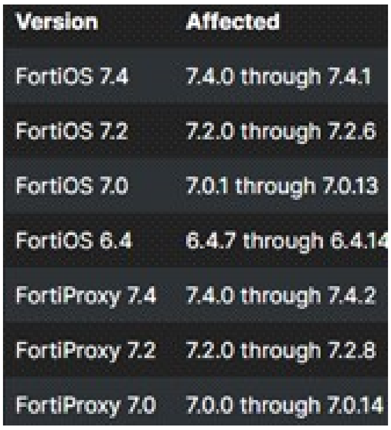
1) Is the metadata in accordance with the vendor advisory (if any) ?
2) Is the metadata current? (if an underlying advisory is updated, is the metadata also ?)
3) Are the CPE’s covering ***all*** affected hardware / software solutions?

Ad 1, about the metadata being in accordance with the vendor advisory: often it is not. Apparently there is still a lot of manual work[16] involved in creating the CVE text. As indicated above, the NVD analyst puts in effort to calculate their own CVSS score, causing discrepancies. The CWE is sometimes also different. But most important: are the CPE’s correct? This is most important, as this is what asset management solutions base their decision on to inform the asset owner about him having a vulnerable product.

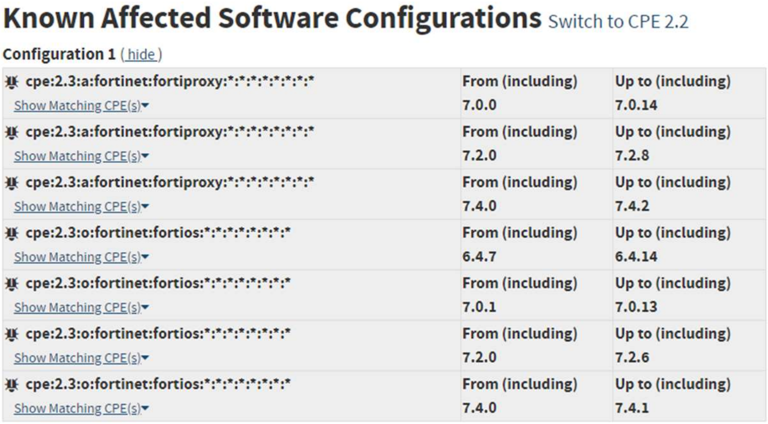
## Correctness

Ad 1, do the CPE’s mention the same affected products and software versions as listed in the original (vendor) advisories? Often they do, but sometimes they don’t. Let’s look at two recent examples for vulnerabilities in FortiNet equipment which caused quite a stir.

**Example 1**
Let’s the CVE-2024-23112. At the left we see what Fortinet mentions, at the right what’s in the CPE’s:



| Version | Affected |
|---|---|
| FortiOS 7.4 | 7.4.0 through 7.4.1 |
| FortiOS 7.2 | 7.2.0 through 7.2.6 |
| FortiOS 7.0 | 7.0.1 through 7.0.13 |
| FortiOS 6.4 | 6.4.7 through 6.4.14 |
| FortiProxy 7.4 | 7.4.0 through 7.4.2 |
| FortiProxy 7.2 | 7.2.0 through 7.2.8 |
| FortiProxy 7.0 | 7.0.0 through 7.0.14 |

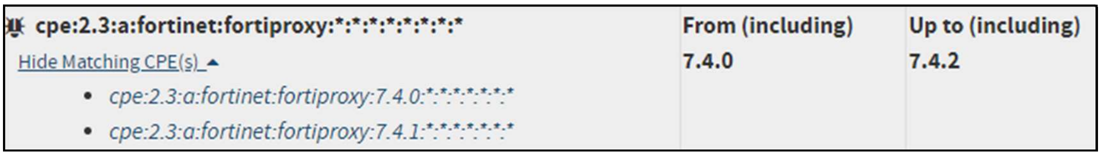


Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 ( hide )

| | | |
|---|---|---|
| cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*<br>Show Matching CPE(s)▾ | From (including)<br>7.0.0 | Up to (including)<br>7.0.14 |
| cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*<br>Show Matching CPE(s)▾ | From (including)<br>7.2.0 | Up to (including)<br>7.2.8 |
| cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*<br>Show Matching CPE(s)▾ | From (including)<br>7.4.0 | Up to (including)<br>7.4.2 |
| cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*<br>Show Matching CPE(s)▾ | From (including)<br>6.4.7 | Up to (including)<br>6.4.14 |
| cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*<br>Show Matching CPE(s)▾ | From (including)<br>7.0.1 | Up to (including)<br>7.0.13 |
| cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*<br>Show Matching CPE(s)▾ | From (including)<br>7.2.0 | Up to (including)<br>7.2.6 |
| cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*<br>Show Matching CPE(s)▾ | From (including)<br>7.4.0 | Up to (including)<br>7.4.1 |

These two perfectly seem match with each other, on first sight. But there is a bug, if one opens the matching CPE details for one of the groups:

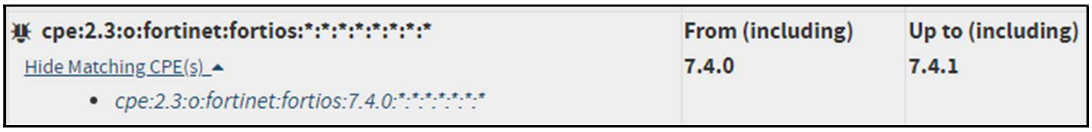


| | | |
|---|---|---|
| cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*<br>Hide Matching CPE(s) ▲<br>• *cpe:2.3:a:fortinet:fortiproxy:7.4.0:*:*:*:*:*:*:*:*<br>• *cpe:2.3:a:fortinet:fortiproxy:7.4.1:*:*:*:*:*:*:*:* | From (including)<br>7.4.0 | Up to (including)<br>7.4.2 |

Is version 7.4.2 forgotten?

[16] *Sometimes even the typo’s in the original text are copy/pasted, indicating that the analyst didn’t completely investigate / understand the issue, and/or the affected products / software versions, and/or the solution.*

**Example 2**
It also happens with the CPE's in CVE-2023-42790, here version 7.4.1 is forgotten to be listed in the matching CPE's:



| cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* | From (including) | Up to (including) |
|---|---|---|
| Hide Matching CPE(s) ▲<br>• cpe:2.3:o:fortinet:fortios:7.4.0:*:*:*:*:*:*:* | 7.4.0 | 7.4.1 |

So I wonder, if CPE's are deemed so important, are they not reviewed? Didn't anyone see this earlier and report it? The result here is that FortiOS 7.4.1 is not flagged as vulnerable, because the CPE is missing. For a vulnerability with a CVSS score 9.3 this is serious.

# Updates

Ad 2, if an underlying (vendor) advisory is changed, is the CVE text and its metadata also updated? It is not uncommon to see a vendor advisory being updated, subsequently listing other, more, or less products / software configurations then were listed in the initial publication[17].

The associated CVE's must then also be updated, which is often done, but not always. Or, it is seen that the CVE text is updated, but the CPE's are not.

**Example**
Siemens advisory "SSA-908185"[18], about an issue in RuggedCOM ROS devices, was updated on November 14, 2023. The associated CVE-2023-24845's change history shows that Siemens (as a CNA) updated the CVE-description itself, adding new vulnerable products.

However, the CPE's were ***not*** updated. This may cause false positives for RuggedCOM devices that have a patch installed, and/or false negatives for devices that had to be mentioned in the CPE's but weren't.

# Completeness

Ad 3, are the CPE's covering *all* affected hardware and software solutions? The answer is: not always. This is often the case for supply-chain components, a common occurrence nowadays.

**Example 1:** Schneider Electric advisory "SEVD-221-313-05"[19], published November 9, 2021 and most recently updated on March 12, 2024 plus twenty more times in-between.

The two CVE's for this so-called "BadAlloc" vulnerability, CVE-2020-35198 and CVE-2020-28895, only refer to the product involved: the VxWorks operating system, and *that product's* CPE's. They do not refer to any Schneider product, and an asset management solution purely based on CPE's would thus 'miss' these vulnerabilities, unless it 'knows' (via SBOM ?) that VxWorks is used inside these Schneider products.

*An asset management tool using the Schneider advisory would not miss these vulnerabilities for more than a hundred (!) Schneider Electric products and product lines.*

**Example 2:** CVE-2021-1392, listing a vulnerability in Cisco IOS switches, summarizes all affected software configurations in the CPE's. But apparently neither the Cisco author nor the NVD analyst was aware that dedicated (and also vulnerable) software versions exist for Rockwell "Stratix" switches, which are internally running Cisco IOS. So an asset owner with vulnerable Stratix switches would not be informed about this vulnerability, based on these CPE's.

*An asset management tool starting using the Rockwell vendor advisory[20] would not miss this vulnerability for Rockwell Stratix switches.*

[17] *I have seen advisories listing hundreds of products, and then it is of course logical that not all patches are published at the same time. Sometimes this takes years.*
[18] *https://cert-portal.siemens.com/productcert/html/ssa-908185.html*
[19] *https://www.se.com/ca/en/download/document/SEVD-2021-313-05/*
[20] *https://www.rockwellautomation.com/en-sg/support/advisory.PN1558.html*

## Summary

The lack of CPE's for OT equipment is quite common, and of increasing concern. This is also true for supply-chain components, whose presence in other products cannot often be detected (perhaps SBOM's can help here in the future).

If the CPE's seen as really important, more attention must be given to their quality (correct, complete and up-to-date). A step in the right direction would be to use an asset management tool that works directly with vendor advisories.

# 5 Enrichment – new sources?

There has already been an announcement of a solution to help solving the NVD gap, like:

- VulnCheck's "NVD++" (https://vulncheck.com/press/vulncheck-nvd)

However it remains to be seen whether private initiatives survive in the long run, given the effort needed to sustain the increasing amount of CVE's. Also, there is probably some moment in the near future where money needs to be made from this NVD++ (NVD usage is free).

If the problems with the NVD persist, I expect more alternatives to develop.

# Summary

The recent inability of the NVD to enrich CVE's is seen by some as an important problem with classifying vulnerabilities. However, in many cases vendor advisories help. They are the "source of truth", are often published quicker than CVE's or ICSA advisories, know directly about the vendor's products (especially of importance for supply-chain issues), and are often more up-to-date than the CVE / CPE / ICSA. This is especially important in the OT space.

A disadvantage is that there is no commonly accepted format for automated ingestion of (OT) vendor advisories, and there is no central location to retrieve these vendor advisories (with the exception of VDE-CERT). Yes there is CSAF and Vuln-O-Gram (and older CVRF), but these are only used by a handful of vendors. For now there is a way to decrease one's reliance on the NVD. Hopefully the crisis within the NVD will help the cyber community to fill the gap quickly.

*This article is likely not complete in discussing all issues related to CPE's.*
*If you have any suggestions, comments or additions, please*
*do not hesitate to contact me (email: rh[at]enodenetworks.com).*