



Everything You Didn't Want to Know About CVE

Paul Asadoorian, Principal Security Evangelist, Eclipsium

<https://eclipsium.com> / <https://securitypodcaster.com>

Scale 1-10 Rank All The Things That Could Go Wrong On Vacation With Kids

Lost Child!

Puke

Illness

Tired

**Lost
Something**

**Broke
Something**

Thirsty

Fighting

Hungry

**Clothing
Malfunction**

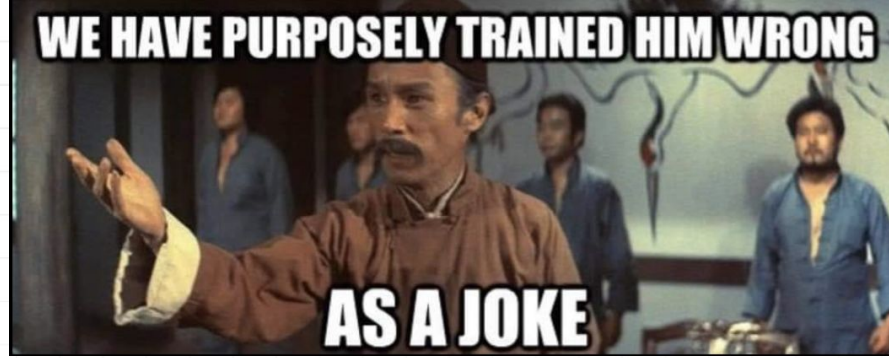
Bathroom

Outline

1. *Problems*

2. *Solutions*





**Problem: CVE Lists The
Wrong Versions As
Vulnerable**

Problem: CVE Lists The Wrong Versions As Vulnerable

- CVEs are created and state which versions are vulnerable. This is an important piece of information!
- **The “all versions up to, and including x.x” statements are not always accurate!**
- In some cases, people get this wrong, which could lead to false positives and false negatives when you are checking to see if you are vulnerable!
- This is common amongst CNAs that deal with Wordpress plugins...

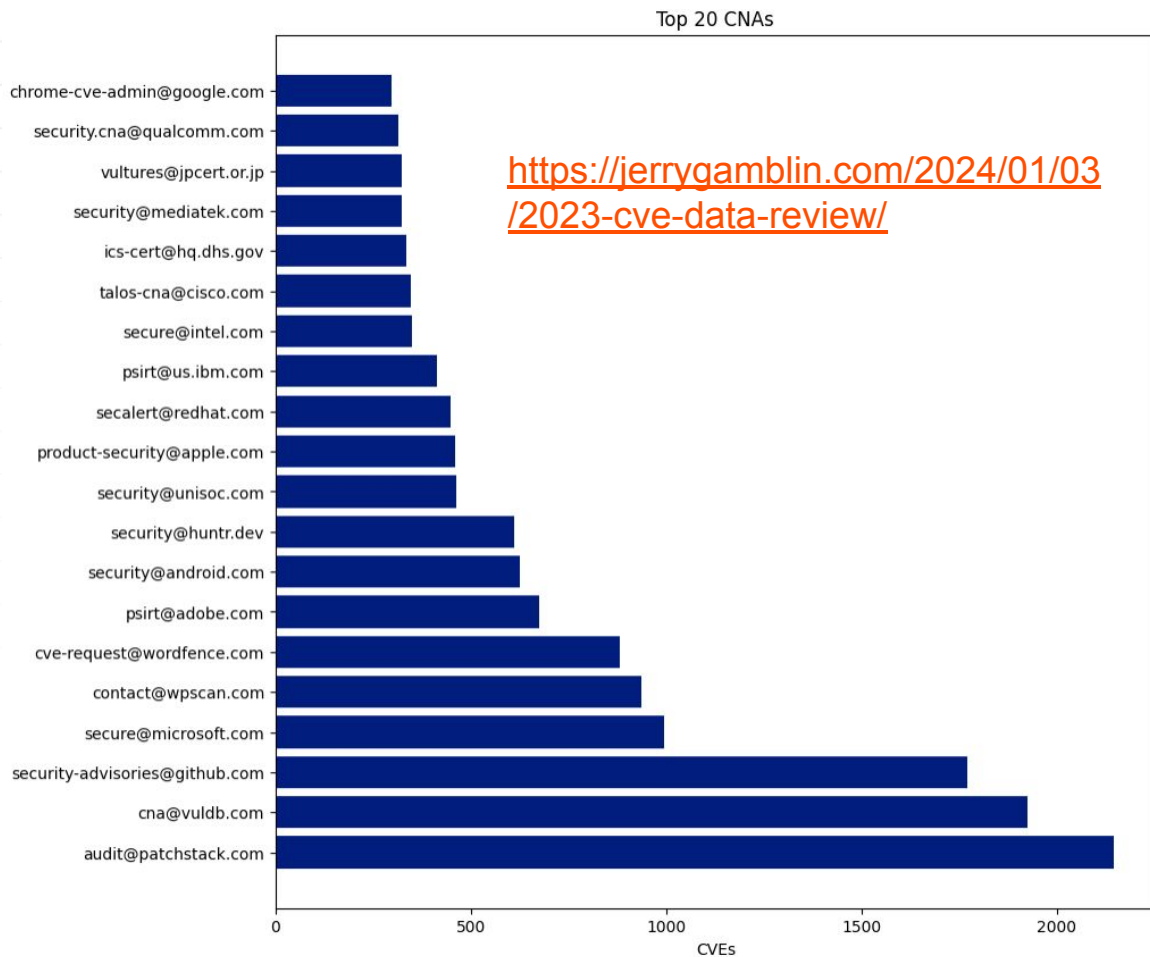
<https://www.pluginvulnerabilities.com/2024/01/22/many-cve-records-are-listing-the-wrong-versions-of-software-as-being-affected/>

WP Plugin	WP Matterport Shortcode	<= 2.1.8	Cross Site Request Forgery (CSRF) vulnerability	4.3	1 day ago
WP Plugin	Convert Post Types	<= 1.4	Cross Site Request Forgery (CSRF) vulnerability	4.3	1 day ago
WP Plugin	Finale Lite	<= 2.18.0	Cross Site Request Forgery (CSRF) vulnerability	4.3	1 day ago
WP Plugin	WP Compress – Image Optimizer [All-In-One]	<= 6.10.35	Cross Site Request Forgery (OSRF) vulnerability	4.3	1 day ago
WP Plugin	ELEX WooCommerce Dynamic Pricing and Discounts	<= 2.1.2	Cross Site Request Forgery (CSRF) vulnerability	4.3	1 day ago
WP Plugin	NextMove Lite	<= 2.18.1	Cross Site Request Forgery (CSRF) vulnerability	4.3	1 day ago
WP Plugin	Easy Logo	<= 1.9.3	Cross Site Scripting (XSS) vulnerability	5.9	1 day ago
WP Plugin	Search Keyword Redirect	<= 1.0	Cross Site Scripting (XSS) vulnerability	5.9	1 day ago
WP Theme	X-T9	<= 1.19.0	Cross Site Request Forgery (CSRF) vulnerability	4.3	1 day ago

<https://patchstack.com/database/>

2023 Top CVE Reporters

Remember: Just because a CVE was reported does not mean the data is accurate or up-to-date!



Problem: Dates Are Confusing



Problem: Dates Can Be Confusing

- Assigned vs Published vs Updated
- The CVE number itself is not reliable to determine when a vulnerability was made public
 - Sometimes the year is from the previous year
 - This could be a pre-allocated CVE number
 - It could also indicate that disclosure took a long time
- We can rely on updated date, but you end up sifting through older CVEs

**Problem:
Anyone Can
Score Using
CVSS**

**In STAR WARS
anyone can hop in
any spaceship and
knows how to fly it.**

**I just spent 20
minutes trying to find
the headlights in a
rental car.**

Problem: Anyone Can Score Using CVSS - LogoFAIL Fail

BRLY-LOGOFAIL-2023-018	DXE Memory Corruption	8.2 (High)	AMI	Acer, Dell, Gigabyte, HP, Intel, Lenovo, MSI, Samsung, Supermicro	CWE-122, CWE-190
------------------------	-----------------------	------------	-----	---	------------------

<https://www.binarly.io/blog/finding-logofail-the-dangers-of-image-parsing-during-system-boot>

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

	NIST: NVD	Base Score: 7.8 HIGH	Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
	CNA: AMI	Base Score: 7.5 HIGH	Vector: CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

<https://nvd.nist.gov/vuln/detail/CVE-2023-39539>

**Problem: Not All
Vulnerabilities
Get A CVE**



Squid Proxy

The majority of these vulnerabilities have not been fixed. All vulnerabilities were discovered in squid-5.0.5. Tests were done in nearly every component possible: forward proxying, reverse proxying, all protocols supports (http, https, https intercept, urn, whois, gopher, ftp), responses, requests, “helpers”, DNS, ICAP, ESI, and caching. Every conceivable possible user and build configuration was used.

<https://www.securityweek.com/dozens-of-squid-proxy-vulnerabilities-remain-unpatched-2-years-after-disclosure/>

FreeRDP

In this blog post we will present the technical details of the attempt to provide a **complete** fix to the root cause of the software vulnerabilities found in FreeRDP, and the timeline of this process. Our case study will be a patch I submitted to the project on **October 2021** and that just recently (Mid-**December 2023**) was announced as part of the latest release ([3.0.0](#)) of the project. Yup, you read it right. The fix was merged **two years ago**, was available on the development branch, and yet it was officially launched only the past few days.

<https://eyalitkin.wordpress.com/2024/01/01/lessons-from-securing-freerdp/>

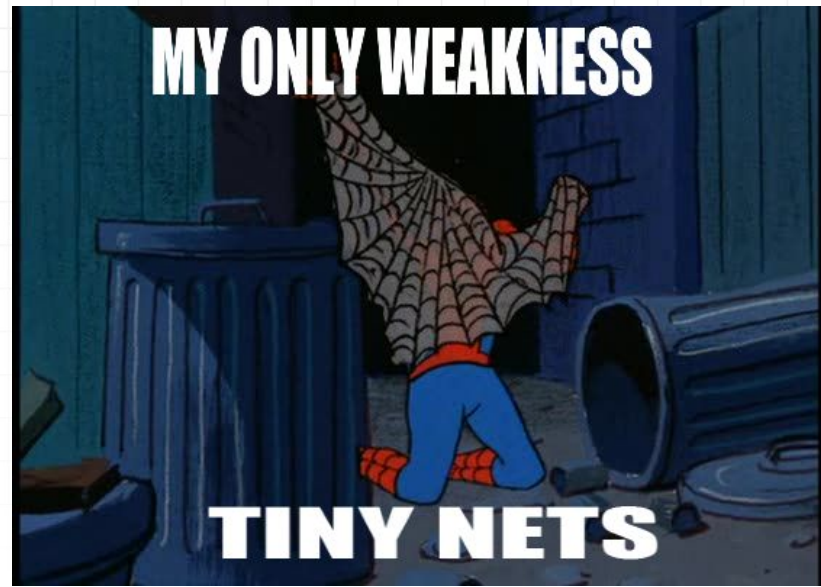
Zyxel

These vulnerabilities are not present in the most recent version of Zyxel firmware (5.37), released last year. Of note, Zyxel has disabled ZTP altogether as of V5.37 patch 1. Eclypsium notified Zyxel of the vulnerabilities but they declined to issue an advisory as the vulnerabilities are not present in the latest version of the firmware. However, since CVEs have not been issued for these vulnerabilities, organizations may not know that they need to update the firmware on their devices. As such, we encourage teams to update their firmware to the latest available version.

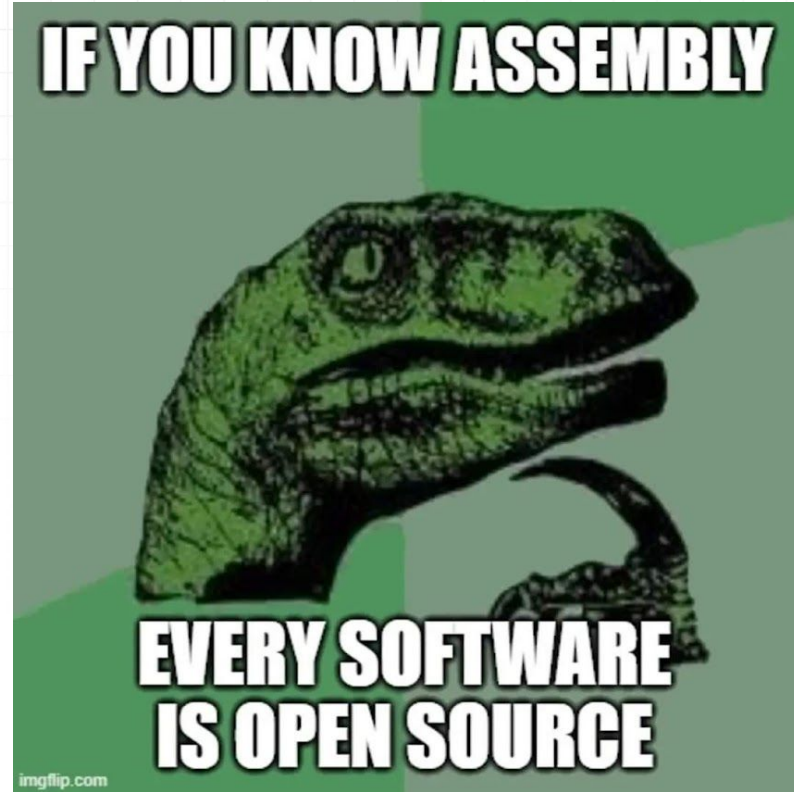
<https://eclypsium.com/blog/dont-play-with-fire-prioritize-zyxel-firewall-update-to-fix-unreported-vulnerability/>

Other Examples

- Weak/Default Passwords
 - Common in IoT and appliances
- Backdoors (sometimes)
 - Backdoors are not secrets?
- Mis-Configurations
 - Introduced by the user
- Unsupported Hardware and Software
 - Again, common in IoT and appliances



**Problem:
Open-Source
Patches Are
Public**



Half Days And More!

Open-source vulnerability disclosure is hard:

- **0-day** - A vulnerability that is unknown to the maintainer of the project.
- **1-day** - A vulnerability that is known to the maintainer. Typically, the CVE is published. There is (typically) an available patch.
- **Half-Day** - Known to the maintainer, information is publicly available (GitHub Commit/PR/Issue), fixes may be in the works, CVE may not be assigned
- **0.75-Day** - Known to the maintainer, patch is available, CVE not assigned or available

Project: <https://github.com/Aqua-Nautilus/CVE-Half-Day-Watcher>

Blog Post: <https://blog.aquasec.com/50-shades-of-vulnerabilities-uncovering-flaws-in-open-source-vulnerability-disclosures>

Problem: Tracking Supply Chain Vulnerabilities Is Hard



CVEs Are For Vulnerabilities - Mostly...

- Who should issue a CVE and for what? - E.g. a vulnerability in a library such as Webp:
 - <https://readme.synack.com/the-problems-with-vulnerability-reporting>
 - <https://www.postgresql.org/about/news/cve-2020-21469-is-not-a-security-vulnerability-2701/>
- Except we got one for XZ: <https://nvd.nist.gov/vuln/detail/CVE-2024-3094> (CWE-506 - Embedded Malicious Code)
- **If we do it for one backdoor, shouldn't we now issue them for all?**



**Problem: How Do We Track
Severity and Impact
Changes?**

This one was a “hoot” ;))

- <https://www.securityweek.com/cisa-says-owl-labs-vulnerabilities-requiring-close-physical-range-exploited-in-attacks/> - It's critical and exploited in the wild! Oh, never mind, it's really not.
- <https://www.shielder.com/blog/2024/01/hunting-for-~~un~~authenticated-n-days-in-asus-routers/> - Unauthenticated remote was only true when running in emulation, actual devices were not as vulnerable.



The Original Severity Changed With:

- **EternalBlue (MS17-010)**: Originally no public exploit for this. The Shadow Brokers group later leaked an exploit developed by the NSA, then WannaCry and NotPetya.
- **BlueKeep (CVE-2019-0708)**: Initially no public exploit for this RDP vulnerability, but later, several researchers and malicious actors developed exploits.
- **Heartbleed (CVE-2014-0160)**: Disclosed in April 2014, but at the time no exploits were publicly known. However, later on researchers and attackers quickly developed exploits that could steal sensitive data from vulnerable servers.
- **Apache Struts CVE-2017-5638**: Disclosed in March 2017. Initially, there was no exploit in the wild, but shortly after the disclosure, attackers began exploiting it to compromise web servers. This vulnerability was notably exploited in the Equifax data breach.
- **Spectre (CVE-2017-5753 and CVE-2017-5715) and Meltdown (CVE-2017-5754)**: These vulnerabilities affect modern microprocessors and were disclosed in January 2018. Initially, there were no known exploits in the wild. However, the disclosure led to a flurry of research and subsequent development of various exploits taking advantage of these hardware vulnerabilities.



Problem: The State of NIST's NVD Program

NIST's NVD Program Needs Love

Summary of what people are saying: We need the enriched CVE data for CVSS and CPE, NIST needs more resources to do this, don't let it fall in the wrong hands.

- <https://resilientcyber.substack.com/p/death-knell-of-the-nvd>
- <https://anchore.com/blog/national-vulnerability-database-opaque-changes-and-unanswered-questions/>
- https://www.linkedin.com/posts/jgamblin_vulnerabilitymanagement-cve-nvd-activity-7172701454816669696-nw00/
- https://www.linkedin.com/posts/netriseinc_cve-vulnerabilitymanagement-cybersecurity-activity-7172030138476388353-mTif/
- https://www.linkedin.com/posts/danlorenc_nvd-nist-fedramp-activity-7172709591091245057-x0lp/



Solutions?



Potential Solutions That Help You With These Problems:

- Do not trust the version number
- Ignore the dates
- Generate your own scores
- Find non-CVE vulnerabilities through intelligence and testing
- Assume there are 0-Days
- Generate your own SBOMs
- Prove something is exploitable (KEV and pen testing)
- Work together to improve CVE, CVSS, EPSS, KEV, etc...

Affected versions and publication dates

```
cve-maker \> critical
```

```
[+] Looking for the latest critical CVEs: ✓
```

CVE	CVSS	Vendor	Product	Description	Update
CVE-2024-3400	10.0			A command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software	
CVE-2023-33045	9.8	QUALCOMM	ar8035	Memory corruption in WLAN Firmware while parsing a NAN management frame carrying a S3 attribute.</td>	2024-04-12
CVE-2023-33028	9.8	QUALCOMM	ar8035	Memory corruption in WLAN Firmware while doing a memory copy of pmk cache.</td>	2024-04-12
CVE-2023-28581	9.8	QUALCOMM	fastconnect_6800	Memory corruption in WLAN Firmware while parsing received GTK Keys in GTK KDE.</td>	2024-04-12
CVE-2023-28562	9.8	QUALCOMM	aqt1000	Memory corruption while handling payloads from remote ESL.</td>	2024-04-12
CVE-2023-28561	9.8	QUALCOMM	qcn7606	Memory corruption in QESL while processing payload from external ESL device to firmware.</td>	2024-04-12
CVE-2023-28543	9.8	QUALCOMM	qcs405	A malformed DLC can trigger Memory Corruption in SNPE library due to out of bounds read, such as by	2024-04-12
CVE-2023-24855	9.8	QUALCOMM	ar8035	Memory corruption in Modem while processing security related configuration before AS Security Exchan	2024-04-12
CVE-2023-22388	9.8	QUALCOMM	315_5g_iot_modem	Memory Corruption in Multi-mode Call Processor while processing bit mask API.</td>	2024-04-12
CVE-2023-22385	9.8	QUALCOMM	315_5g_iot_modem	Memory Corruption in Data Modem while making a MO call or MT VOLTE call.</td>	2024-04-12
CVE-2023-21631	9.8	QUALCOMM	205	Weak Configuration due to improper input validation in Modem while processing LTE security mode comm	2024-04-12
CVE-2022-40537	9.8	QUALCOMM	apq8009	Memory corruption in Bluetooth HOST while processing the AVRC_PDU_GET_PLAYER_APP_VALUE_TEXT AVRCP re	2024-04-12
CVE-2022-40515	9.8	QUALCOMM	apq8009	Memory corruption in Video due to double free while playing 3gp clip with invalid metadata atoms.</t	2024-04-12
CVE-2022-40514	9.8	QUALCOMM	aqt1000	Memory corruption due to buffer copy without checking the size of input in WLAN Firmware while proce	2024-04-12
CVE-2022-40510	9.8	QUALCOMM	apq8009	Memory corruption due to buffer copy without checking size of input in Audio while voice call with E	2024-04-12
CVE-2022-33279	9.8	QUALCOMM	ar9380	Memory corruption due to stack based buffer overflow in WLAN having invalid WNM frame length.</td>	2024-04-12
CVE-2022-33259	9.8	QUALCOMM	mdm8207	Memory corruption due to buffer copy without checking the size of input in modem while decoding raw	2024-04-12
CVE-2022-33256	9.8	QUALCOMM	ar8035	Memory corruption due to improper validation of array index in Multi-mode call processor.</td>	2024-04-12
CVE-2022-33211	9.8	QUALCOMM	mdm8207	memory corruption in modem due to improper check while calculating size of serialized CoAP message</	2024-04-12
CVE-2022-25745	9.8	QUALCOMM	mdm9205	Memory corruption in modem due to improper input validation while handling the incoming CoAP message	2024-04-12

```
cvemap -s critical -f kev,poc
```

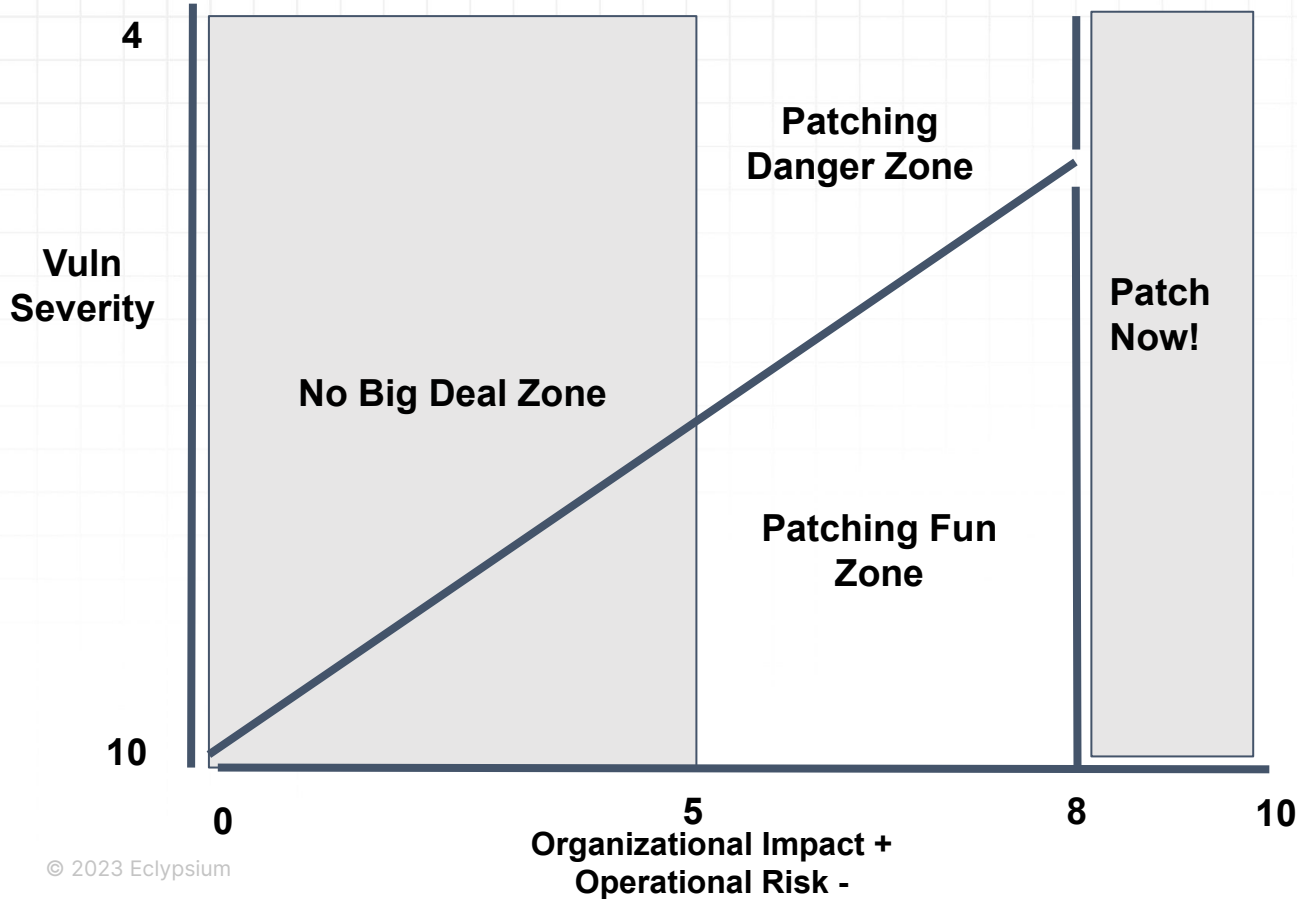


projectdiscovery.io

[INF] Current cvemap version v0.0.6 (latest)

ID	CVSS	SEVERITY	EPSS	PRODUCT	AGE	TEMPLATE	KEV	POC
CVE-2024-3400	9.8	CRITICAL	0.00043			×	FALSE	FALSE
CVE-2024-3272	9.8	CRITICAL	0.00177		8	×	TRUE	TRUE
CVE-2024-31997	9.9	CRITICAL	0.00045		1	×	FALSE	FALSE
CVE-2024-31996	10	CRITICAL	0.00044		1	×	FALSE	FALSE
CVE-2024-31988	9.6	CRITICAL	0.00044		1	×	FALSE	FALSE
CVE-2024-31987	9.9	CRITICAL	0.00045		1	×	FALSE	FALSE
CVE-2024-31986	9	CRITICAL	0.00045		1	×	FALSE	FALSE
CVE-2024-31984	9.9	CRITICAL	0.00044		1	×	FALSE	FALSE
CVE-2024-31983	9.9	CRITICAL	0.00045		1	×	FALSE	FALSE
CVE-2024-31982	10	CRITICAL	0.00045		1	×	FALSE	FALSE
CVE-2024-31981	9.9	CRITICAL	0.00045		1	×	FALSE	FALSE
CVE-2024-31849	9.8	CRITICAL	0.00043		6	×	FALSE	TRUE
CVE-2024-31848	9.8	CRITICAL	0.00043		6	×	FALSE	TRUE
CVE-2024-31465	9.9	CRITICAL	0.00044		1	×	FALSE	FALSE
CVE-2024-31461	9.1	CRITICAL	0.00045		1	×	FALSE	FALSE

Paul's Vulnerability Patching Matrix



Generate your own scores!

Find non-CVE vulnerabilities through intelligence and testing

- Use threat and vulnerability feeds (open-source and commercial options exist)
- Subscribe to PTAS (Pen Testing As A Service) and ASM (Attack Surface Management) services
- Monitor feeds on your own (I have tips for you!)

Exploit Feeds 352

0day.today 45

CXSECURITY Databa... 19

CXSECURITY Databa... 19

Exploit Files ≈ Packet ... 67

Exploit-DB.com RSS ... 28

Exploitalert 19

inTheWild.io Exploitati... 4

Spl0itus.com Exploits... 150

The Exploit Database ... 1

5 more feeds

Vuln Feeds 703+

GitHub Advisory Data... 154

Open Source Security 214

VU Updates 3

VulDB Updates 250+

Vulners 12

ZDI: Published Adviso... 70

GitHub Advisory Database

5K followers / 64 articles per week / #security #security-advisories

LATEST

[GHSA-4wh3-3wf2-39m9] Summernote vulnerable to cross-site scripting GitHub Security Advisory: G

[GHSA-qjx3-2g35-6hv8] Mautic Sensitive Data Exposure due to inadequate user permission settings

[GHSA-4vwx-54mw-vqfw] Traefik vulnerable to denial of service with Content-length header

[GHSA-9fcx-cv56-w58p] Mautic vulnerable to Relative Path Traversal / Arbitrary File Deletion due to

[GHSA-6363-v5m4-fvq3] timber/timber vulnerable to Deserialization of Untrusted Data 3 TTPs

[GHSA-fpw7-j2hg-69v5] mysql2 Remote Code Execution (RCE) via the readCodeFor function

[GHSA-jjg7-2v4v-x38h] Internationalized Domain Names in Applications (IDNA) vulnerable to denial

[GHSA-x565-32qp-m3vf] phin may include sensitive headers in subsequent requests after redirect

[GHSA-wm4w-7h2q-3pf7] Matrix IRC Bridge truncated content of messages can be leaked

[GHSA-95pr-fxf5-86gv] Cosign malicious artifacts can cause machine-wide DoS

[GHSA-88jx-383q-w4qc] Cosign malicious attachments can cause system-wide denial of service

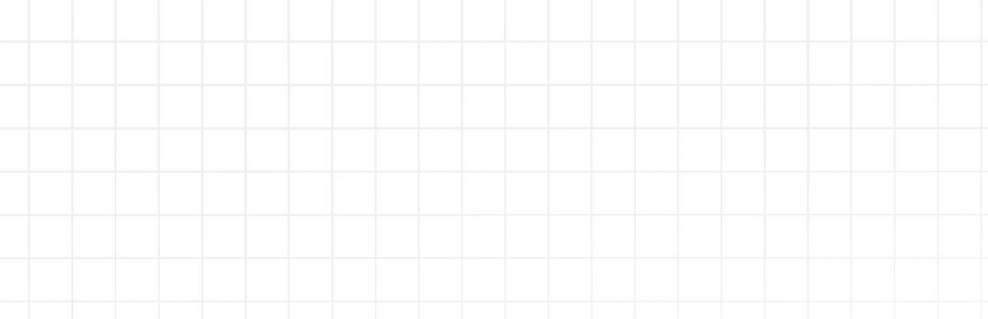
[GHSA-37q5-v5qm-c9v8] Transformers Deserialization of Untrusted Data vulnerability 2 TTPs

[GHSA-j85q-46hg-36p2] SpiceDB: LookupSubjects may return partial results if a specific kind of rel

[GHSA-3f95-mxq2-2f63] Gradio Local File Inclusion vulnerability Exploitation for Client Execution

[GHSA-46cm-pfwy-cqf8] LiteLLM has Server-Side Template Injection vulnerability in /completions e





What do you want to name this AI feed?

Appliances

Track specific companies, products, and topics across the web

Cisco × F5 × Fortinet × Citrix Systems ×

Ivanti × Juniper Networks × Palo Alto Networks ×

Check Point × + OR

- Appliances 2
- AI Appliances 2
- Advisories Archive - Ch...
- Checkpoint Advisories
- FortiGuard Labs | FortiG...
- Ivanti Blog: Security Adv...
- Juniper Security Advisor...
- Palo Alto Networks Sec...

Appliances

1 follower / 98 articles per week

LATEST

- Attackers exploit critical zero-day flaw in Palo Alto Networks firewalls Palo Alto Networks •
- Palo Alto Networks discloses critical vulnerability in its firewall operating system Palo Alto Networks •
- CVE-2024-3400: Zero-Day Vulnerability in Palo Alto Networks PAN-OS GlobalProtect Gateway Exploited in the Wild
- CERTFR-2024-ALE-006 : Vulnérabilité dans Palo Alto Networks PAN-OS (12 avril 2024) Palo Alto Networks •

Looking For Half-Day Vulnerabilities

```
$ python scan_nvd.py --github_token `cat token.txt` \  
  
--days 10 \  
  
--min_stars 500  
  
https://services.nvd.nist.gov/rest/json/cves/2.0/?pubStartDate=2024-04-02T18:17:56&pubEndDate=2024-04-13T18:17:56&resultsPerPage=2000  
  
found a possible half_day on CVE-2023-29483 with the reference:  
  
https://github.com/rthalley/dnspython/issues/1045
```

Cheet Sheet Time!

1. Use an RSS Reader - Download my OPML file here:
 - a. [PaulsFeeds.opml](#)
2. Use cve-maker (<https://github.com/msd0pe-1/cve-maker>)
 - a. `python3 -m cve-maker`
 - b. `critical` - To get the latest critical CVEs
 - c. `search <keyword>` - Searches the CVE database for keyword
 - d. `get <CVE-ID>` - Gets info about the CVE and lists any exploits
3. Use cvemap (<https://github.com/projectdiscovery/cvemap>):
 - a. go install github.com/projectdiscovery/cvemap/cmd/cvemap@latest
 - b. `cvemap -age 20 -s critical -f kev,poc` - Get the last 20 days of CVEs, only those that are 9.0 CVSS or above, indicate if its in the CISA KEV and if there is a PoC exploit available
4. Use CVE Half Day Watcher (<https://github.com/Aqua-Nautilus/CVE-Half-Day-Watcher>):
 - a. [Create a Github API token](#)
 - b. `python scan_nvd.py --github_token `cat token.txt` --days 10 --min_stars 500` - Scan Github for "Half Day" vulnerabilities in the past 10 days, filtering only Github projects with more than 500 stars

Assume there are 0-Days

Go out and get the latest, next generation, AI enhanced, multi-layered, cutting-edge, 0-Day threat protection solution on the market...

Then, throw it away

Then, implement a solid infosec strategy and plan (different talk)

Don't mind me, just taking out the trash

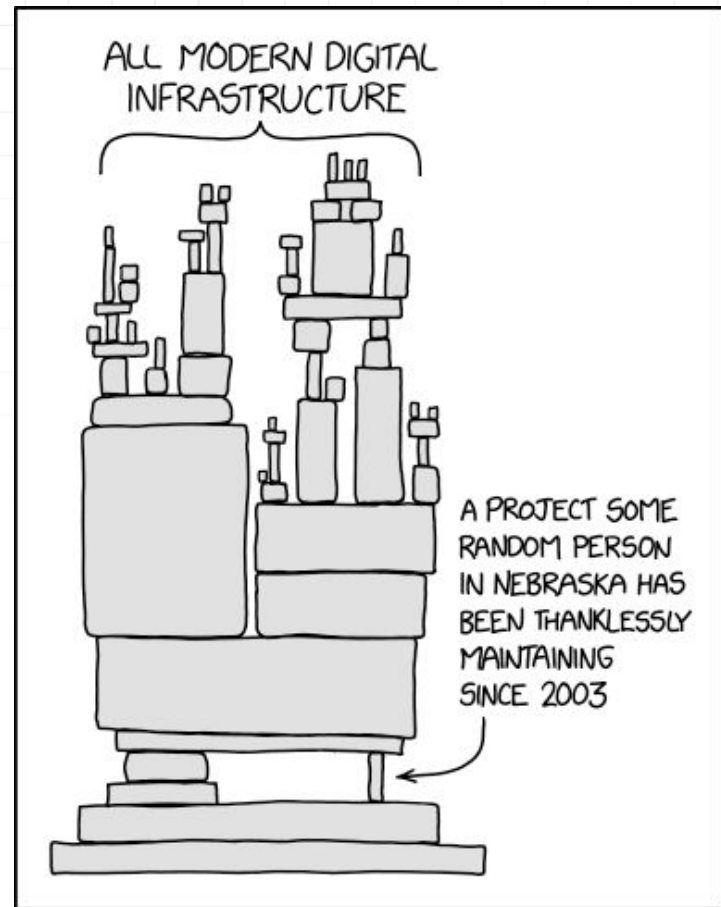


Generate your own SBOMs

- Firmware: <https://github.com/e-m-b-a/emba>
- Containers: <https://anchore.com/sbom/how-to-generate-an-sbom-with-free-open-source-tools/>
- Java: <https://github.com/CycloneDX/cyclonedx-maven-plugin>
- General: <https://github.com/microsoft/sbom-tool>

Use Google's OSV

- <https://blog.hartwork.org/posts/expat-2-6-2-released/>
- <https://osv.dev/vulnerability/CVE-2024-28757>
- <https://google.github.io/osv.dev/faq/>
- Discover open-source dependencies and related vulnerabilities



- <https://xkcd.com/2347/>

Prove something is exploitable (KEV and pen testing)

```
cve-maker \> search firmware
```

```
[+] Looking for the latest firmware CVEs: ✓
```

CVE	CVSS	Vendor	Product	Description	Update
CVE-2023-33061	7.5	QUALCOMM	ar8035	Transient DOS in WLAN Firmware while parsing WLAN beacon or probe-response frame.</td>	2024-04-12
CVE-2023-33056	7.5	QUALCOMM	ar8035	Transient DOS in WLAN Firmware when firmware receives beacon including T2LM IE.</td>	2024-04-12
CVE-2023-33048	7.5	QUALCOMM	ar8035	Transient DOS in WLAN Firmware while parsing t2lm buffers.</td>	2024-04-12
CVE-2023-33047	7.5	QUALCOMM	ar8035	Transient DOS in WLAN Firmware while parsing no-inherit IES.</td>	2024-04-12
CVE-2023-33045	9.8	QUALCOMM	ar8035	Memory corruption in WLAN Firmware while parsing a NAN management frame carrying a S3 attribute.</td>	2024-04-12
CVE-2023-33028	9.8	QUALCOMM	ar8035	Memory corruption in WLAN Firmware while doing a memory copy of pmk cache.</td>	2024-04-12
CVE-2023-33027	7.5	QUALCOMM	315_5g_iot_modem	Transient DOS in WLAN Firmware while parsing rsn ies.</td>	2024-04-12
CVE-2023-33026	7.5	QUALCOMM	ar8035	Transient DOS in WLAN Firmware while parsing a NAN management frame.</td>	2024-04-12
CVE-2023-33016	7.5	QUALCOMM	csr8811	Transient DOS in WLAN firmware while parsing MLO (multi-link operation).</td>	2024-04-12
CVE-2023-33015	7.5	QUALCOMM	315_5g	Transient DOS in WLAN Firmware while interpreting MBSSID IE of a received beacon frame.</td>	2024-04-12
CVE-2023-28581	9.8	QUALCOMM	fastconnect_6800	Memory corruption in WLAN Firmware while parsing received GTK Keys in GTK KDE.</td>	2024-04-12
CVE-2023-28563	5.5	QUALCOMM	aq11000	Information disclosure in IOE Firmware while handling WMI command.</td>	2024-04-12
CVE-2023-28561	9.8	QUALCOMM	qcn7606	Memory corruption in QESL while processing payload from external ESL device to firmware.</td>	2024-04-12
CVE-2023-28539	7.8	QUALCOMM	ar8035	Memory corruption in WLAN Host when the firmware invokes multiple WMI Service Available command.</td>	2024-04-12
CVE-2023-24854	7.8	QUALCOMM	215	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.</td>	2024-04-12
CVE-2023-24851	7.8	QUALCOMM	ar8035	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.</td>	2024-04-12
CVE-2023-21660	7.5	QUALCOMM	csr8811	Transient DOS in WLAN Firmware while parsing FT Information Elements.</td>	2024-04-12
CVE-2023-21659	7.5	QUALCOMM	315_5g_iot_modem	Transient DOS in WLAN Firmware while processing frames with missing header fields.</td>	2024-04-12
CVE-2023-21658	7.5	QUALCOMM	ar8035	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.</td>	2024-04-12
CVE-2023-21656	7.8	QUALCOMM	ar8035	Memory corruption in WLAN HOST while receiving an WMI event from firmware.</td>	2024-04-12

```
[+] Looking ExploitDB exploits for firmware: ✓
```

EDB	language	Description	Author	Release Date	Update
EDB-44381	text	Tenda FH303/A300 Firmware v5.07.68_EN - Remote DNS Change	Todor Donev	2018-03-30	2018-04-02
EDB-40081	python	Belkin AC1200 Router Firmware 1.00.27 - Authentication Bypass	Gregory Smiley	2016-07-11	2016-07-11
EDB-20654	perl	APC WEB/SNMP Management Card (9606) Firmware 3.0 - Telnet Administration Denial of Service	altomo	2001-02-26	2012-08-20
EDB-27942	text	AVTECH DVR Firmware 1017-1003-1009-1003 - Multiple Vulnerabilities	Core Security	2013-08-29	2013-08-29
EDB-51269	python	Arris Router Firmware 9.1.103 - Remote Code Execution (RCE) (Authenticated)	Yerodin Richards	2023-04-06	2023-04-06

Work together to improve CVE, CVSS, EPSS, KEV, etc...

- I believe these are all great programs
- I do not believe we want to see them replaced by commercial offerings or run by commercial companies 100%
- Much of the issues stem from lack of funding and resources
- We can help with the resources part!

Good News

- Microsoft adopts CWE
 - <https://msrc.microsoft.com/blog/2024/04/toward-greater-transparency-adopting-the-cwe-standard-for-microsoft-cves/>
 -
- What if there is no patch available for EOL products?
- I LOVE this: *“Separate critical security fixes for customers and not bundle those patches with new product features or functionality changes.”*
 - <https://www.centerforcybersecuritypolicy.org/insights-and-research/network-resilience-coalition-offers-recommendations-for-improving-network-infrastructure-security-in-new-white-paper>
 -
- EPSS Improvements: <https://www.cyentia.com/epss-report/>

Thank You!

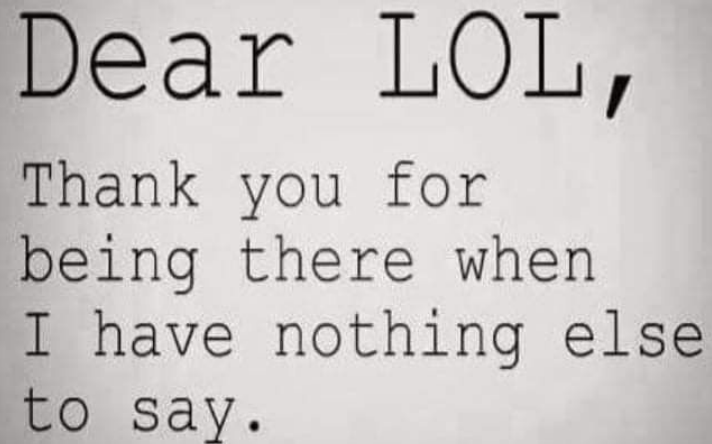
Presentations referenced in this presentation are here:

<https://securitypodcaster.com/presentations/>

Contact me: <https://securitypodcaster.com/contact/>

Subscribe to my podcasts:

<https://securitypodcaster.com/podcasts/>



Dear LOL,
Thank you for
being there when
I have nothing else
to say.