This is the Big One!

...right?

Me. Vs. The Big Vulnerability

Me. Vs. The Big Vulnerability

‹ Blog Home

CVE-2021-44228: Apache Log4j2 Zero-Day Exploited in the Wild (Log4Shell)

SECURITY

Log4Shell - Detecting Log4j 2 RCE Using Splunk

The Rise of “Branded” Vulnerabilities

Media in category "Security vulnerability logos"

The following 41 files are in this category, out of 41 total.

Badlock logo.svg
283 × 283; 2 KB

BlueKeep logo.svg
512 × 371; 2 KB

Breach Attack logo.svg
598 × 110; 5 KB

CacheOut logo.png
4,739 × 4,204; 227 KB

CacheOut logo.svg
512 × 454; 11 KB

CCS Injection.svg
512 × 512; 1 KB

DirtyCow.svg
415 × 475; 375 KB

DROWN logo.svg
307 × 306; 4 KB

Efail logo.svg
283 × 283; 30 KB

Espectro logo con texto.svg
702 × 836; 28 KB

Evil32.png
1,174 × 2,366; 16 KB

Foreshadow logo with narrow text.svg
512 × 512; 7 KB

Foreshadow logo with wide text.svg
512 × 512; 7 KB

Foreshadow logo without text.svg
512 × 512; 5 KB

FragAttacks.png
823 × 918; 84 KB

Heartbleed.svg
567 × 678; 2 KB

Httpoxy.svg
512 × 132; 34 KB

KRACK-logo-small.png
644 × 819; 104 KB

Light Commands.png
2,000 × 2,000; 166 KB

Meltdown code logo.svg
572 × 236; 56 KB

Meltdown logo with text.svg
512 × 996; 6 KB

Meltdown logo without text.png
2,048 × 3,344; 182 KB

Meltdown logo without text.svg
512 × 836; 4 KB

Openssl-CVE-2016-6304.svg
512 × 512; 2 KB

ProxyLogon logo - Black.png
1,501 × 1,401; 1.6 MB

ProxyLogon logo - White.png
1,501 × 1,401; 1.69 MB

Rambleed-10.svg
512 × 452; 8 KB

Robotattack.svg
668 × 1,290; 8 KB

Security Policy.png
250 × 259; 33 KB

Spectre and Intel logos combined.png
297 × 202; 24 KB

Basic Idea

There are **Bad** Vulnerabilities

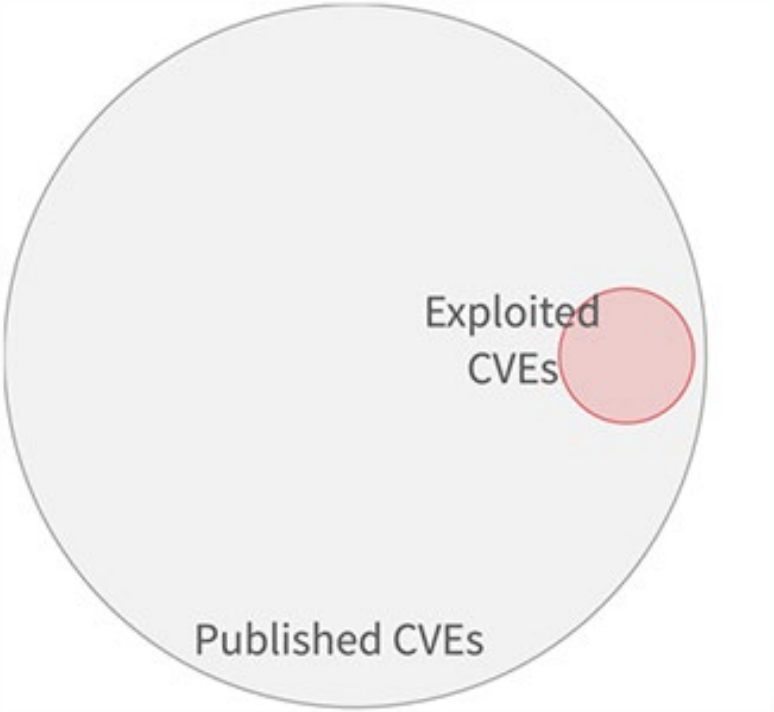
There are **Loud** Vulnerabilities

And there are some that are **Bad** *and* **Loud**

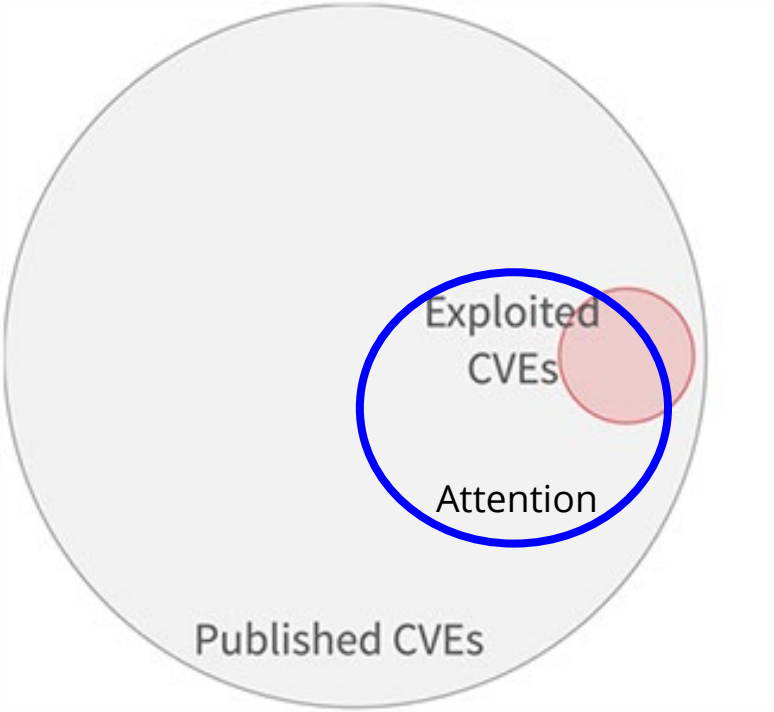
Attention is a limited resource.

We want to optimize *attention* against *risk.* How are we doing?

Basic Idea



Basic Idea



Defining Terms

Badness:

- EPSS - (Point in Time)
  - >.9 (as of 8-22-23 pull)
- Known Exploited Vulnerabilities (CISA) - KEV

Attention:

- Google Trends - Point in time (and buggy)
- Google Search Results (how many results you'd get now)
- NVD References

Badness vs. Attention

Defining Attention

Google Trends

- Measured at a point in time
- Relative to some benchmark amount
- Only 5 terms at a time

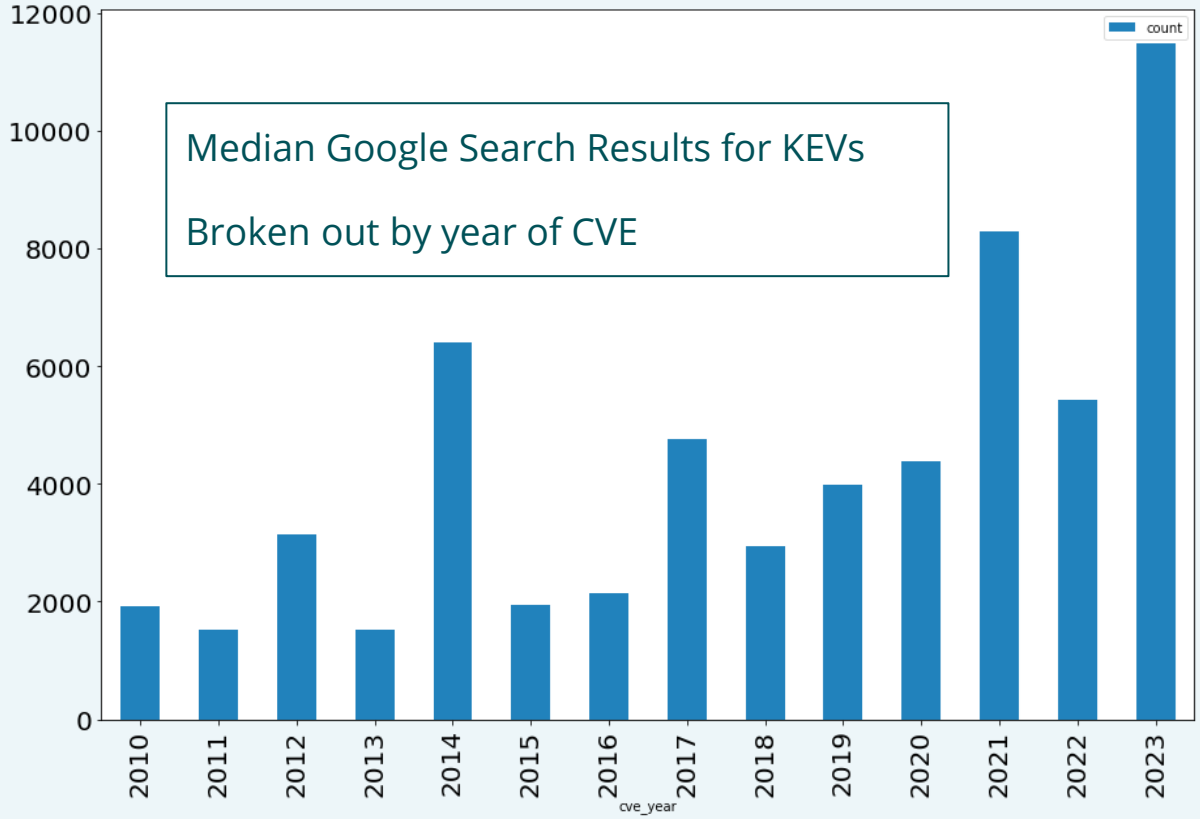
Search Results

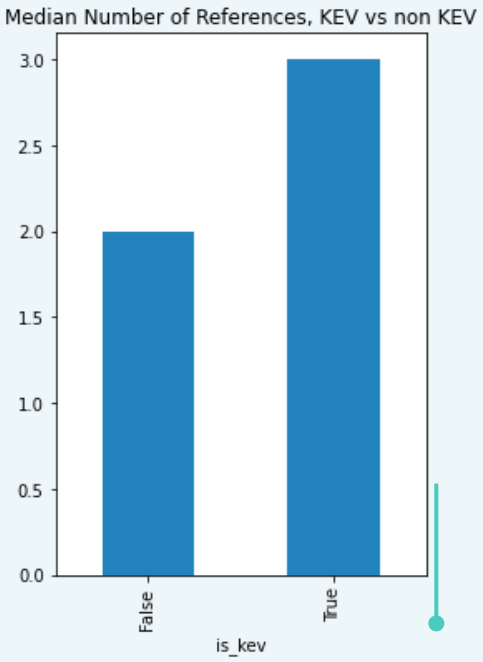
- Measured as if you searched today
- Can limit to keyword matching
- Rate limited

CVE References

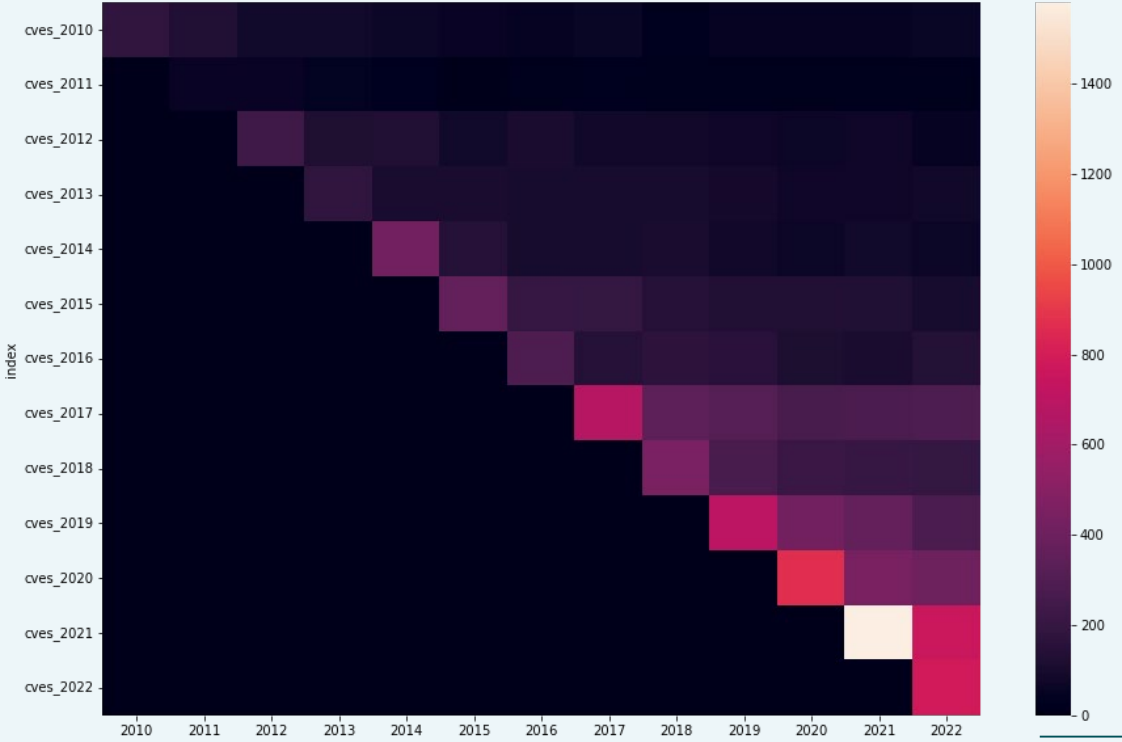
- Vendors
- US Gov

We’re paying more attention!

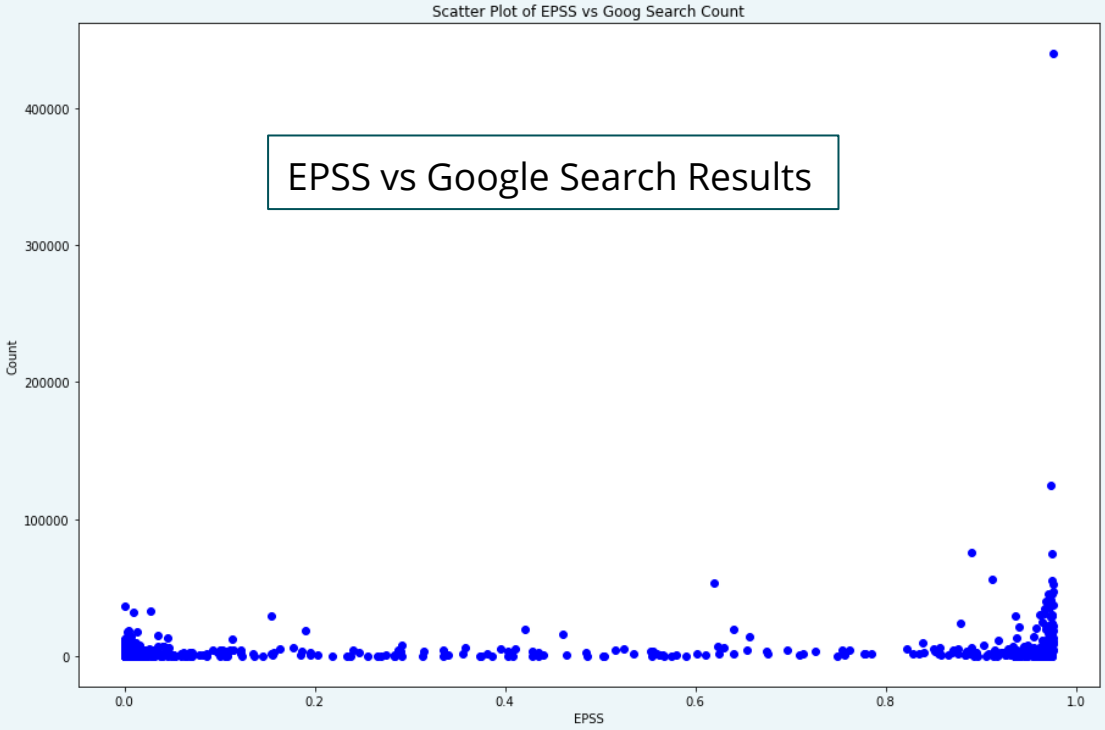




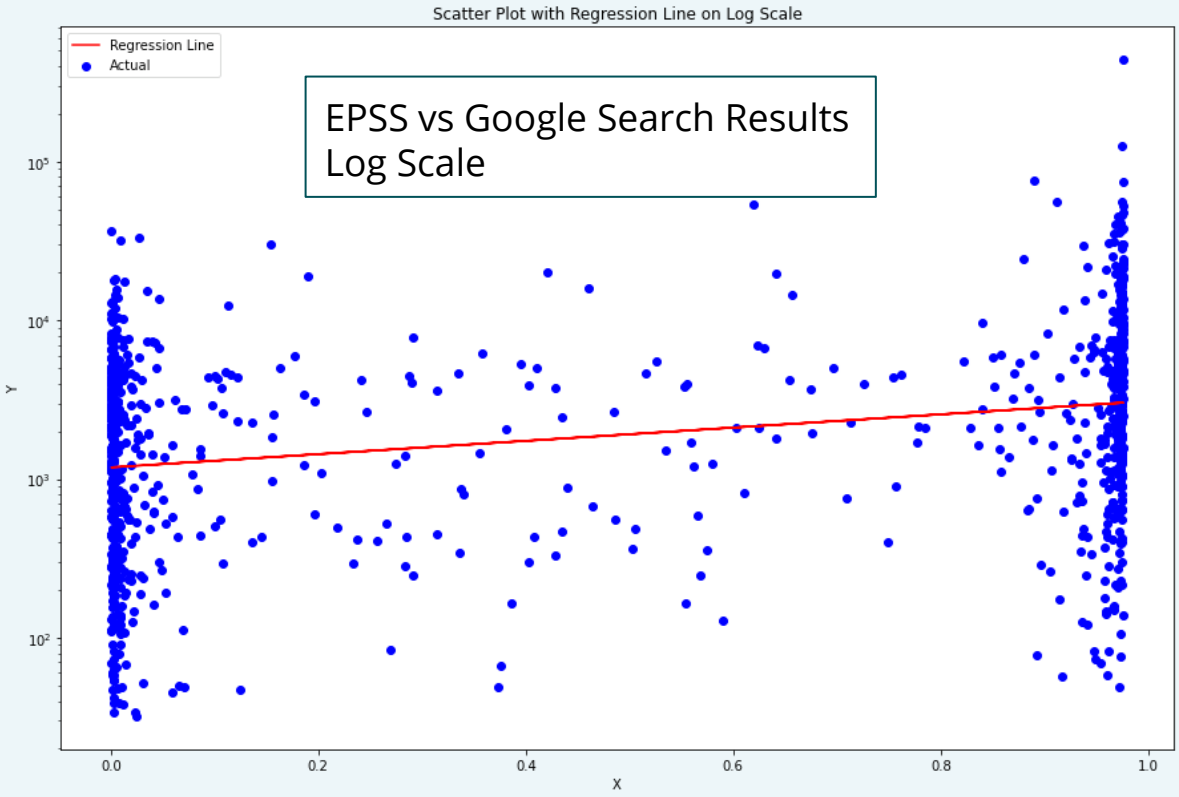
We’re paying more attention - sooner!



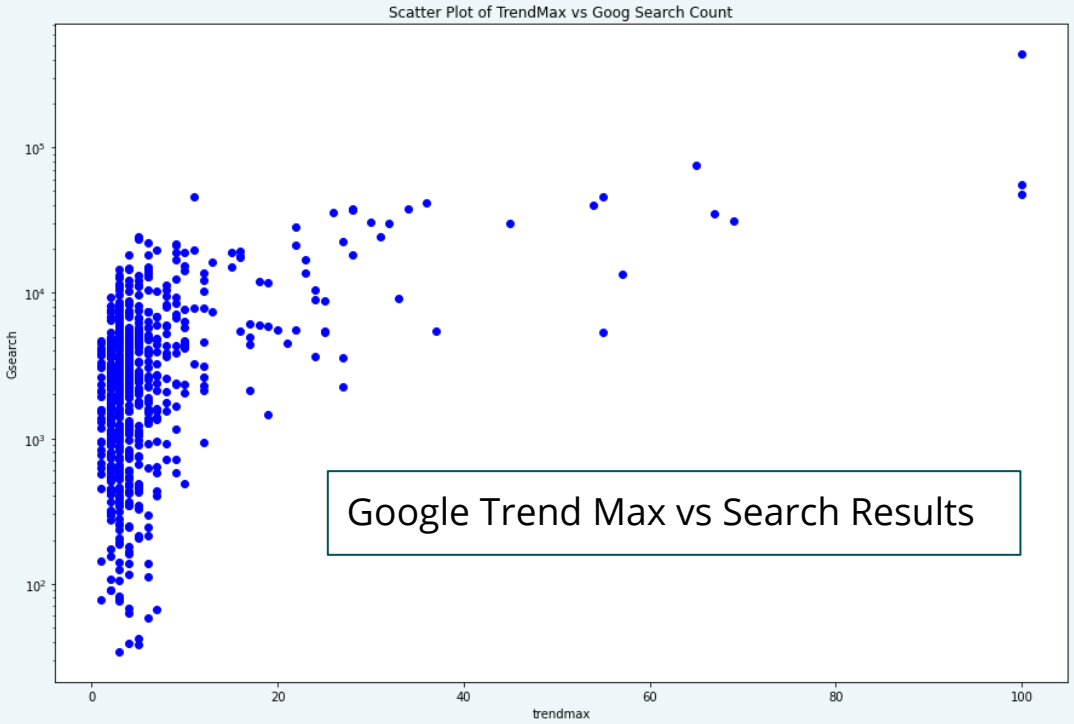
Does Attention Correlate with EPSS?



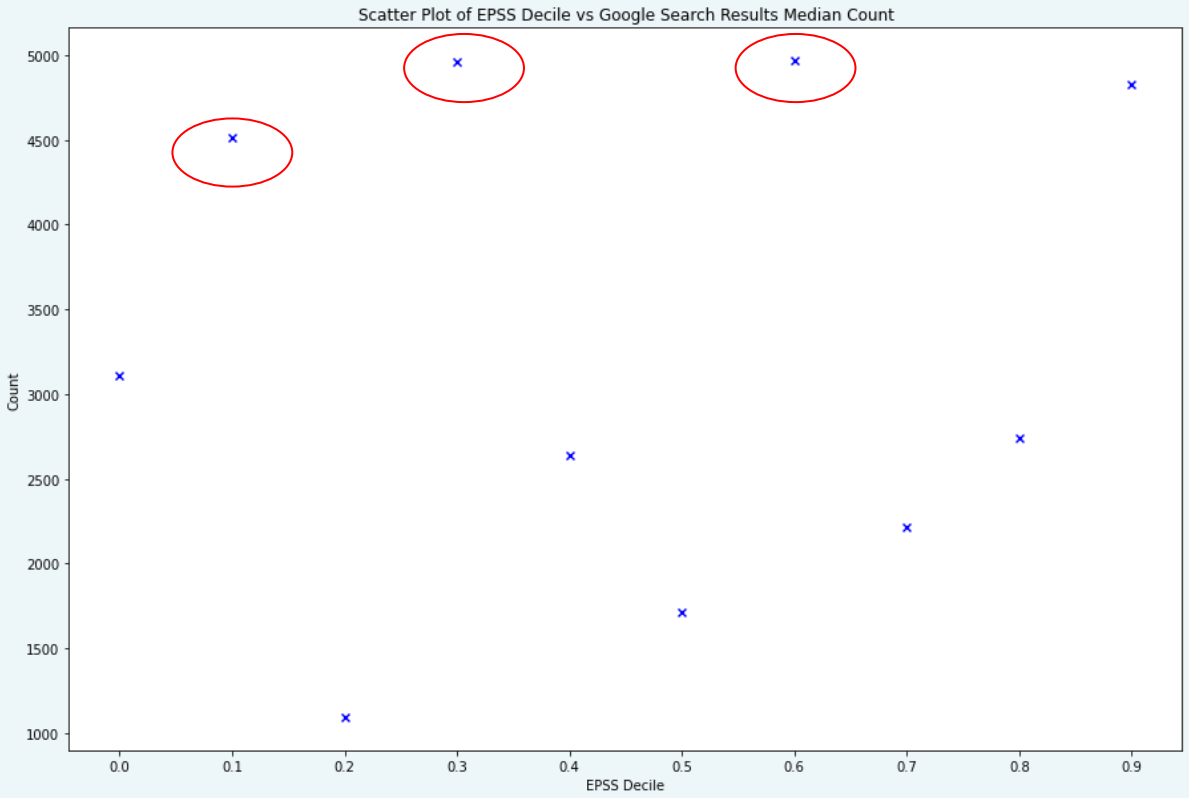
Log Scale


Scatter Plot with Regression Line on Log Scale
Regression Line
Actual
EPSS vs Google Search Results
Log Scale
10^5
10^4
10^3
10^2
Y
0.0
0.2
0.4
0.6
0.8
1.0
X

Trendiness vs Total search Results (KEV only)



Ok but what about recently?



What are we not paying attention to but maybe should?

Google Search # < 20%

EPSS >= .9

44 CVEs in KEV

- More obscure products
- Older

```
forgottens['vendorProject'].value_counts()
✓ 0.0s
```

Microsoft	8
D-Link	4
NETGEAR	4
Adobe	4
Unraid	2
Oracle	2
Google	2
Tenda	2
Delta Electronics	1
Atlassian	1
Arcserve	1
Cisco	1
Kentico	1
Arm	1
D-Link and TRENDnet	1
Zoho	1
Nagios	1
Quest	1
Citrix	1
IBM	1
rConfig	1
Aviatrix	1
LG	1
SAP	1

```
forgottens['year'].value_counts()
✓ 0.0s
```

2017	8
2021	7
2020	7
2019	5
2013	5
2018	4
2016	3
2015	2
2022	1
2012	1
2010	1

What are we paying too much attention to?

Google Results above 80% percentile

EPSS < .2

- Newer
- More mainstrea
- Security Cos

```
overrated['vendorProject'].value_counts()
```

✓ 0.0s

Google	5
Microsoft	4
Apple	3
Linux	2
Ivanti	1
Fortinet	1
Palo Alto Networks	1
WebRTC	1
Barracuda Networks	1
Red Hat	1
Meta Platforms	1

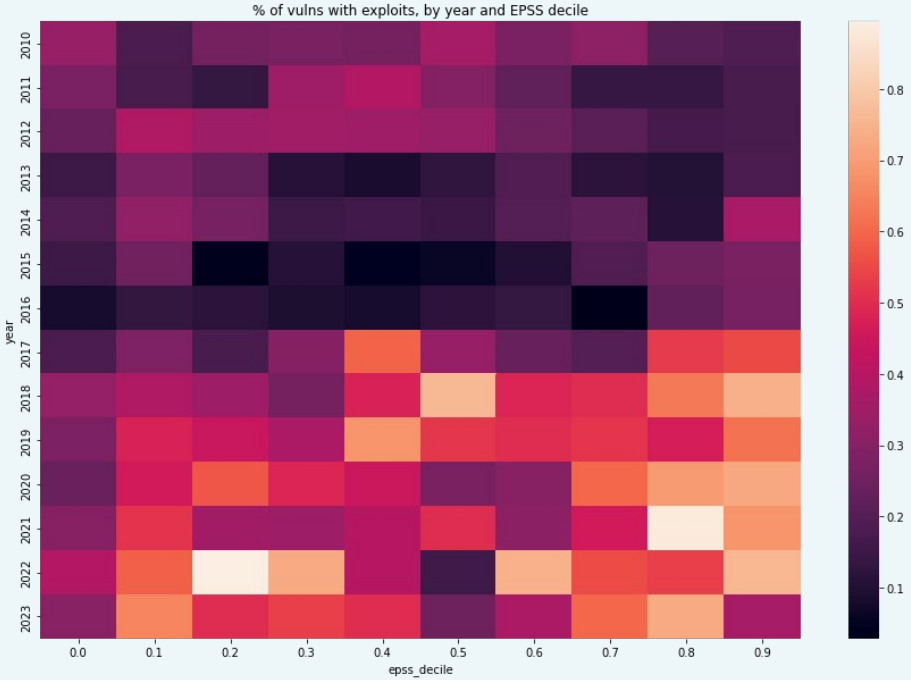
```
overrated['year'].value_counts()
```

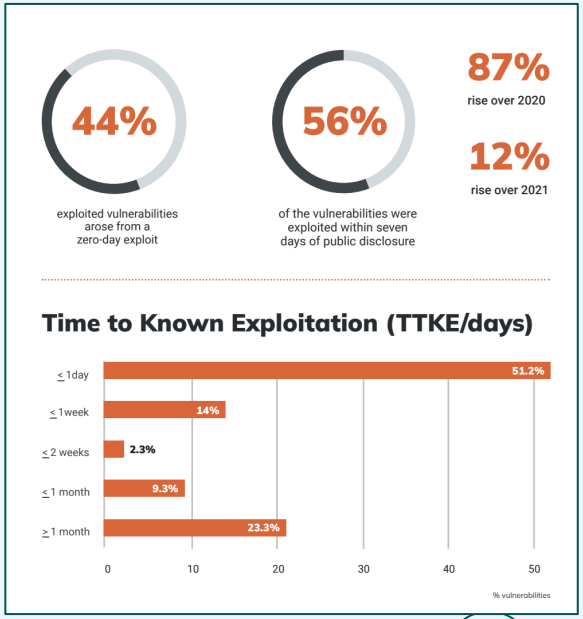
✓ 0.0s

2023	12
2022	5
2020	2
2019	2

Corresponding Trends

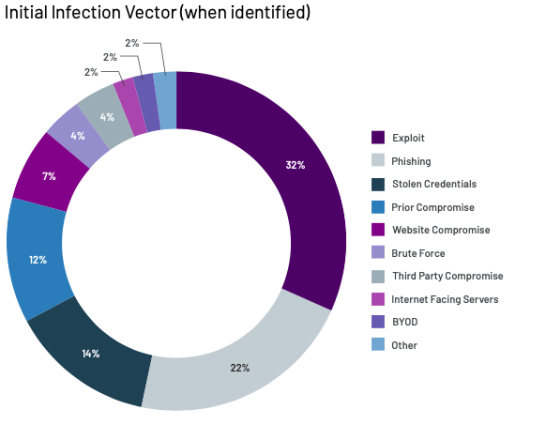
Are attackers (and researchers) building exploits faster?





Are attackers using more server side exploits? -

The State of the Threat Report from Secureworks found that cyber vulnerability exploitation in remote services has become the primary initial access vector (IAV) in ransomware attacks over the past year, accounting for 52% of ransomware incidents and overtaking the top spot from credential-based attacks from 2021.



What's up with in-the-wild exploits? Plus, what we're doing about it.

March 10, 2022

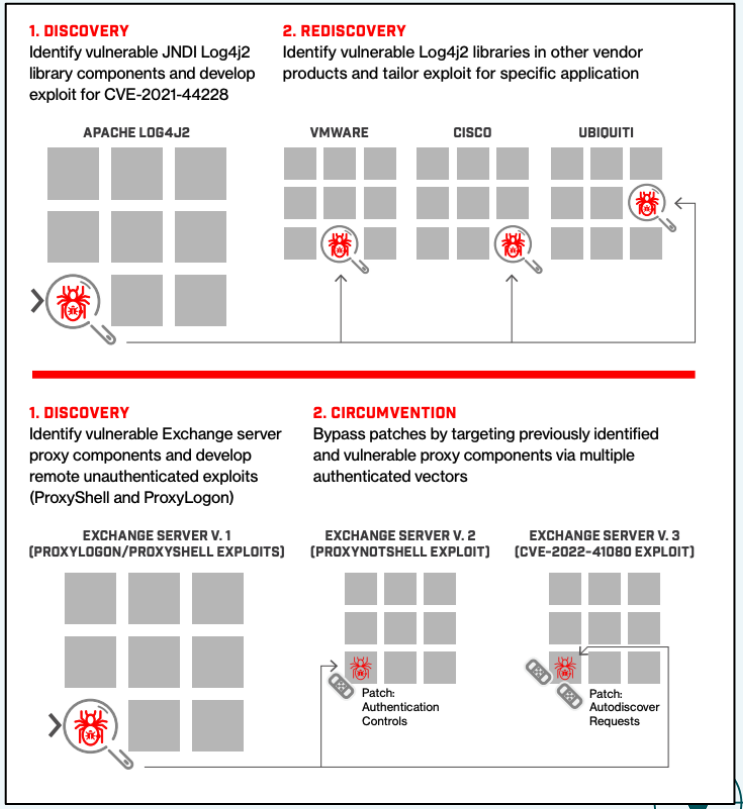
Posted by Adrian Taylor, Chrome Security Team

If you are a regular reader of our Chrome release blog, you may have noticed that phrases like 'exploit for CVE-1234-567 exists in the wild' have been appearing more often recently. In this post we'll explore why there seems to be such an increase in exploits, and clarify some misconceptions in the process. We'll then share how Chrome

Shoutout

"These growing nation-state attacks coincided with organizations struggling to manage an explosive landscape of vulnerabilities that amplified systemic risk.

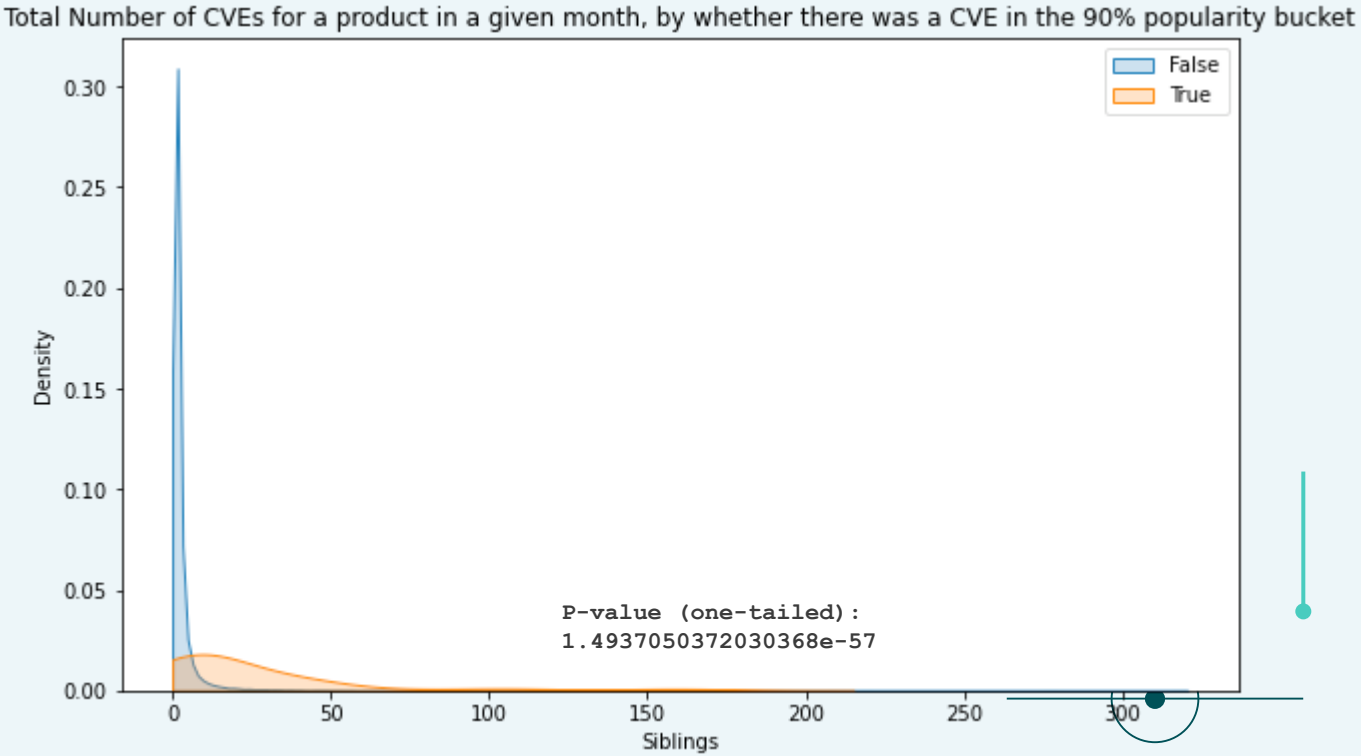
The constant disclosure of vulnerabilities affecting legacy infrastructure like Microsoft Active Directory continued to burden security teams and present an open door to attackers, while the ubiquitous Log4Shell vulnerability ushered in **a new era of "vulnerability rediscovery," during which adversaries modify or reapply the same exploit to target other similarly vulnerable products."**



https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf

Do Popular Vulns Bring More Vulns?

CVEs are so fetch



Examples

ProxyLogon
March 2021: CVE-2021-27065
Microsoft Exchange Server Remote Code Execution Vulnerability (HAFNIUM Exploited)

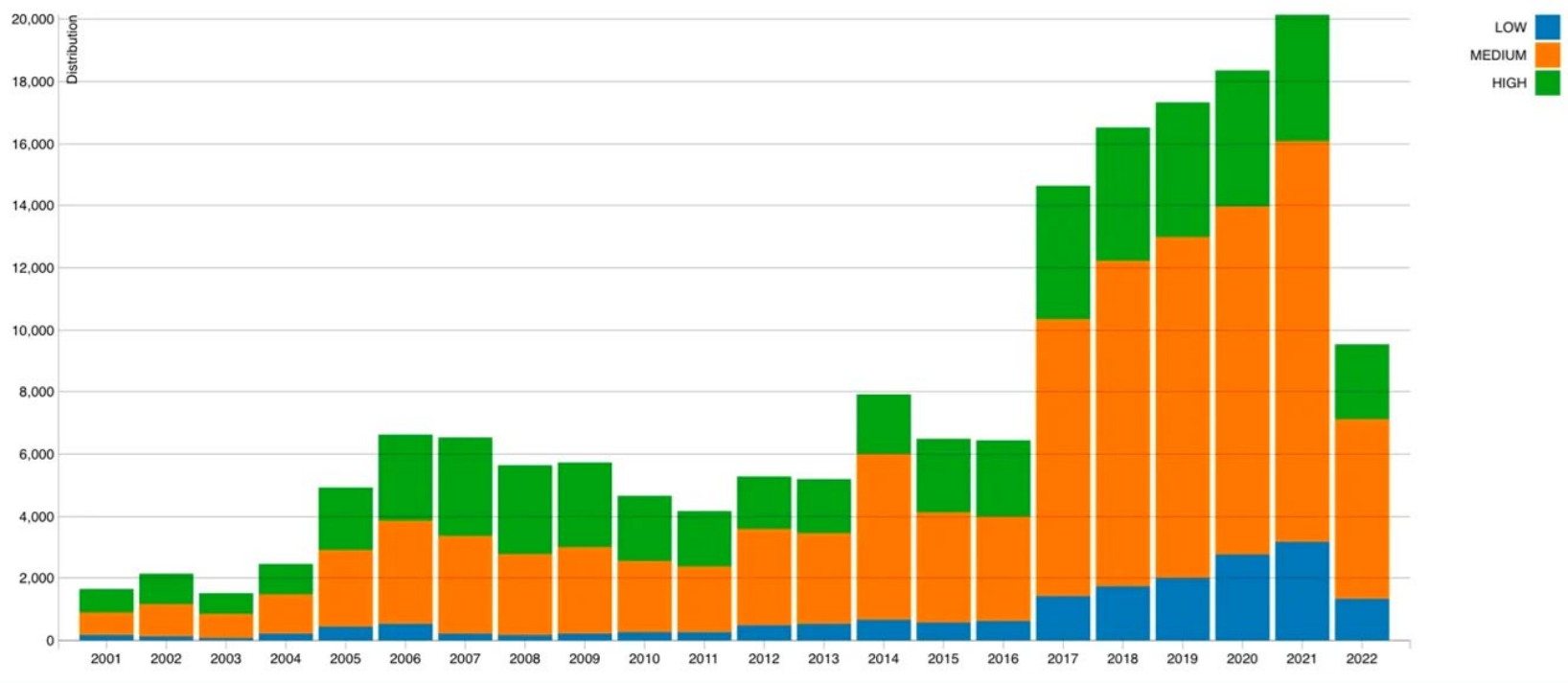
Adobe:
July 2018: CVE-2018-4993, CVE-2018-4979
Adobe Acrobat Pro DC URL Parsing Insufficient Verification of Data Authenticity Information Disclosure Vulnerability

Oracle:
January 2020: CVE-2020-2551, CVE-2020-2555

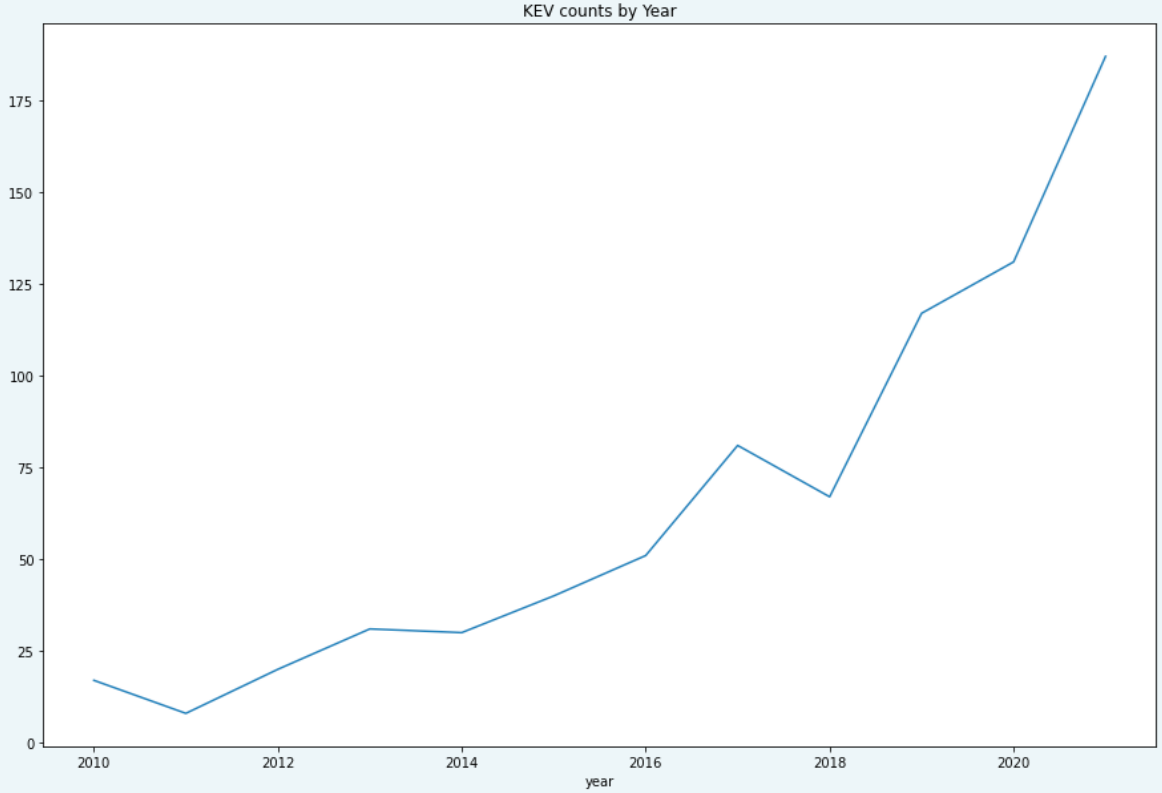
CVE-2020-2551: Unauthenticated RCE In Oracle WebLogic

Wild Speculation

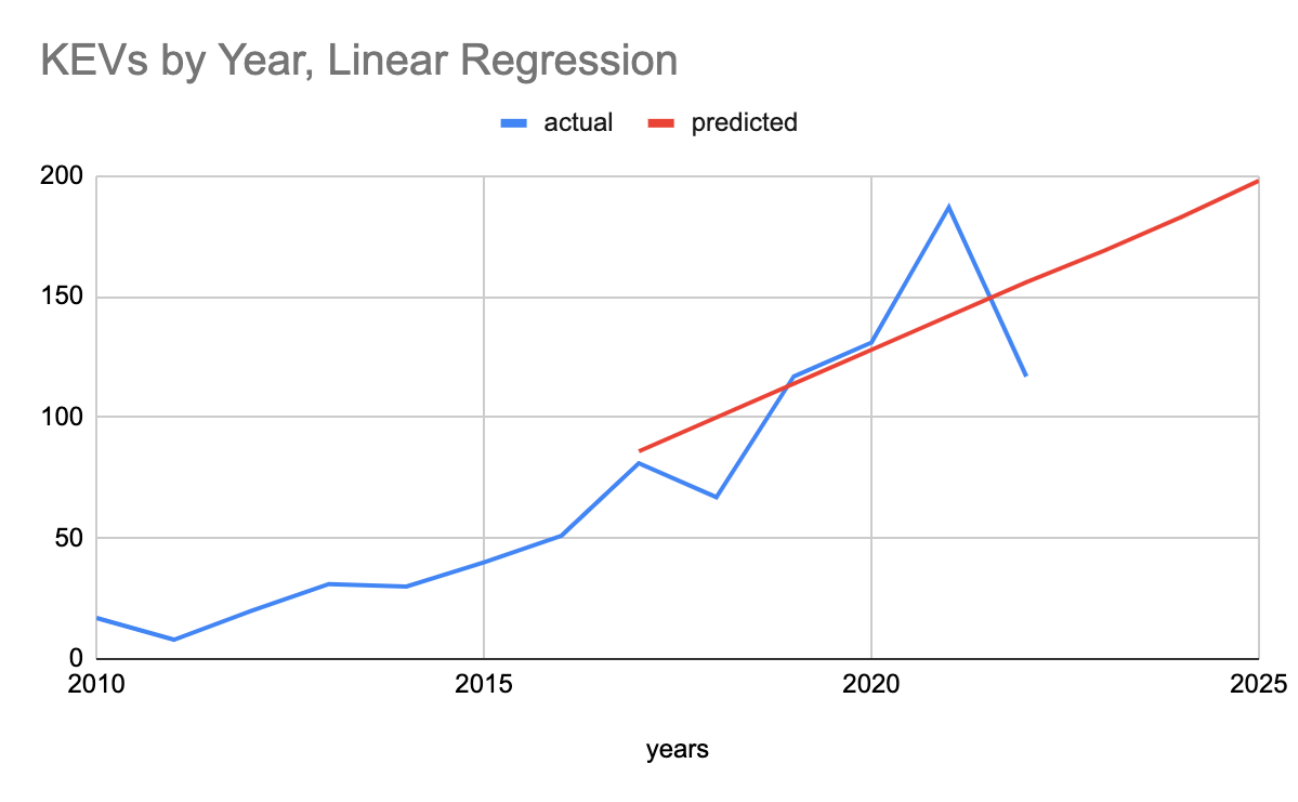
More Vulns = More Bad Vulns



Finally: Let’s Forecast



KEVs in 2023, 2024

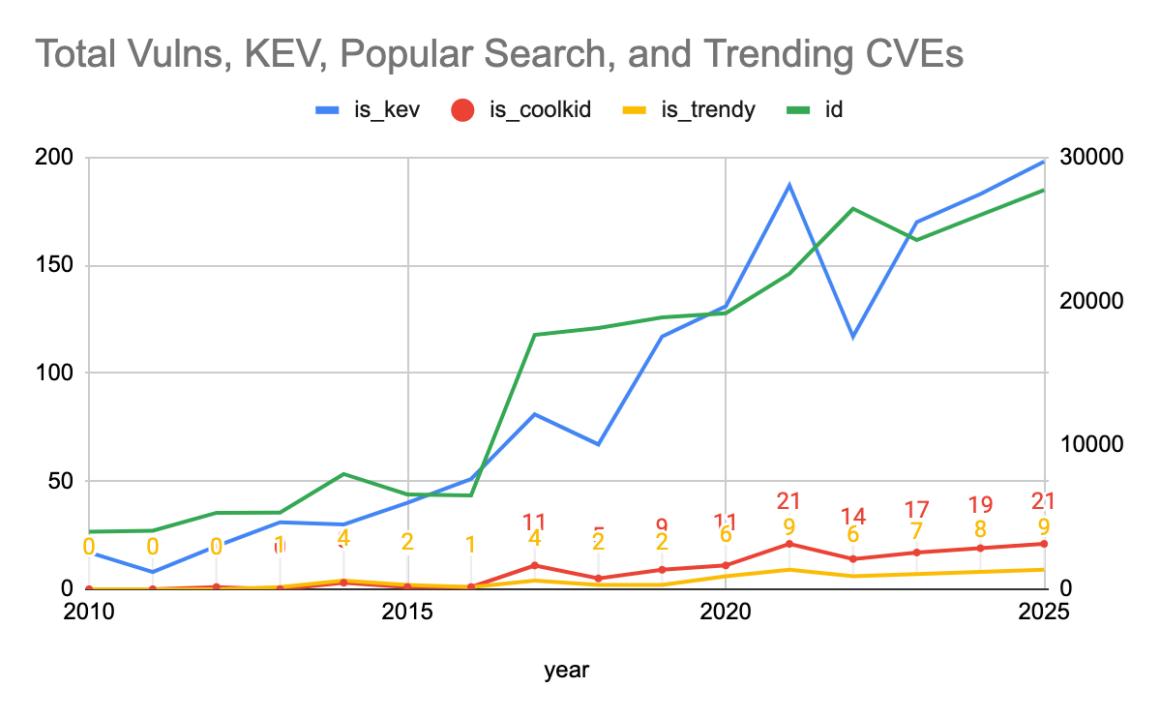


Predictions:

2023 KEVs = 169
2024 KEVs = 183

Predicting Headliners

How many headliners can we expect next year?



Predictions:

Coolkid = lots of search results

Trendy = Spike in interest

2023 CK = 17
2024 CK = 19

2023 Trendy = 7
2024 Trendy = 8

In Summary

More Vulns

Sheer volume means more bad ones

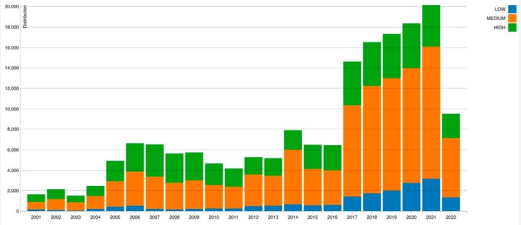
More Attention

Attention breeds more vulns

Faster Exploit Turnaround

And Attackers seem to be using them more

In Summary



More Vulns

Sheer volume means more bad ones

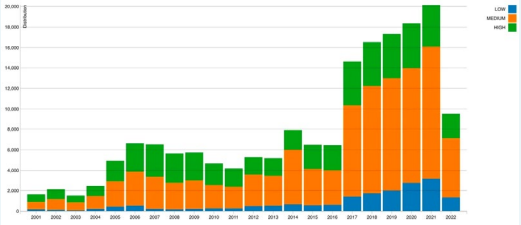
More Attention

Attention breeds more vulns

Faster Exploit Turnaround

And Attackers seem to be using them more

In Summary



More Vulns

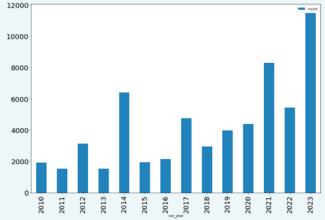
Sheer volume means more bad ones

More Attention

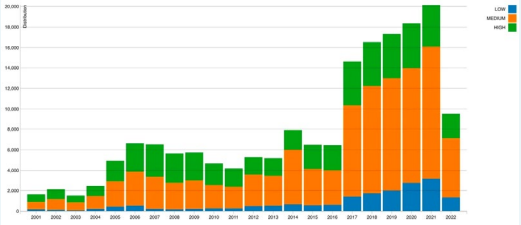
Attention breeds more vulns

Faster Exploit Turnaround

And Attackers seem to be using them more



In Summary



More Vulns

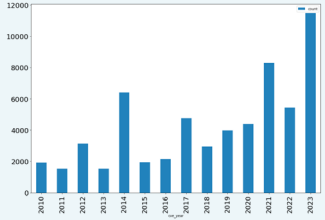
Sheer volume means more bad ones

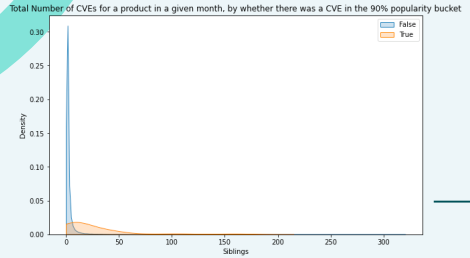
Faster Exploit Turnaround

And Attackers seem to be using them more

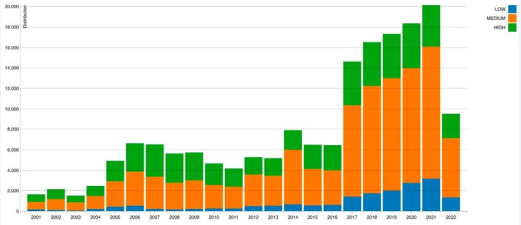
More Attention

Attention breeds more vulns



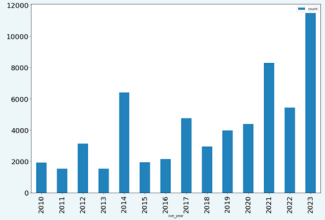


In Summary



More Vulns

Sheer volume means more bad ones

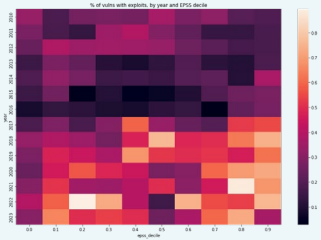


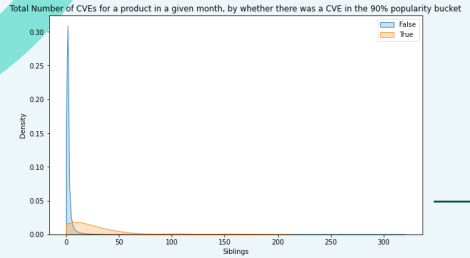
Faster Exploit Turnaround

And Attackers seem to be using them more

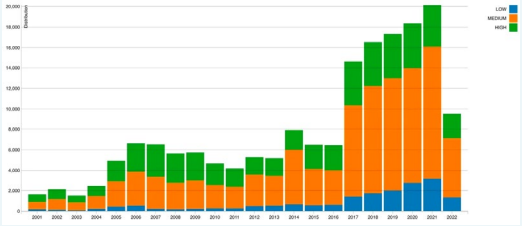
More Attention

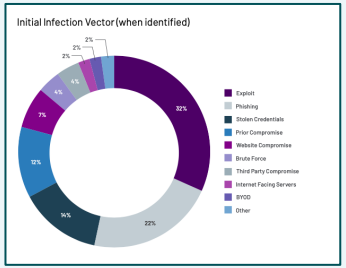
Attention breeds more vulns





In Summary





More Vulns

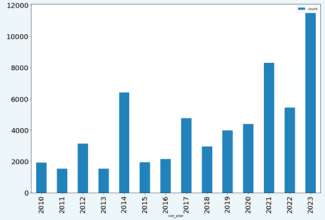
Sheer volume means more bad ones

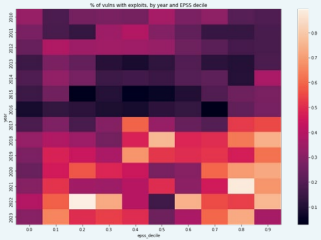
Faster Exploit Turnaround

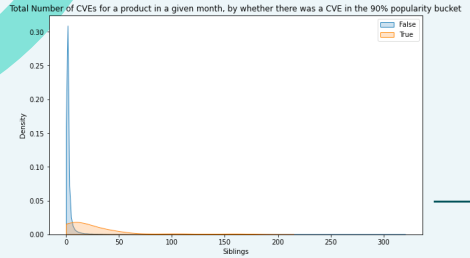
And Attackers seem to be using them more

More Attention

Attention breeds more vulns







There is Hope

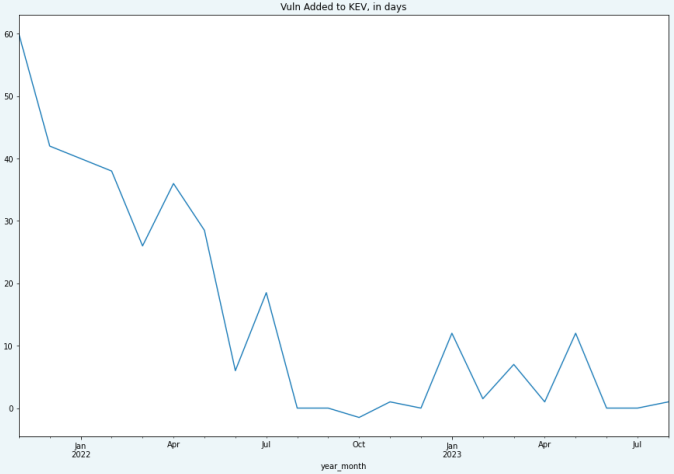
Against increased speed of disclosure and exploitation, we also need to increase speed of prioritization and action.

There is Hope

Against increased speed of disclosure and exploitation, we also need to increase speed of prioritization and action.

KEV updating faster

Good Job, KEV!

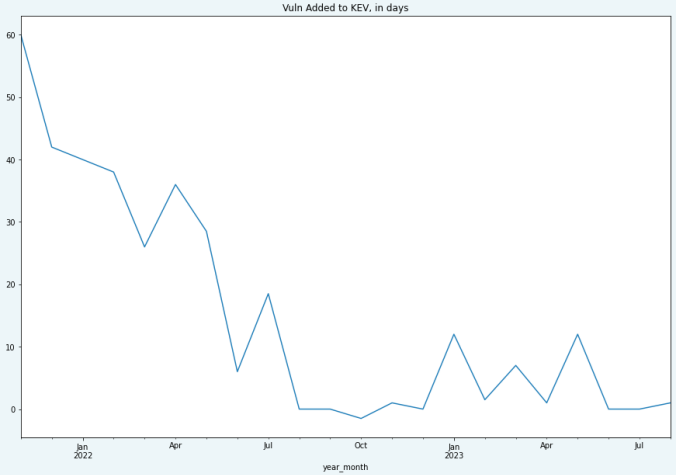


In The Future

Against increased speed of disclosure and exploitation, we also need to increase speed of prioritization and action.

KEV updating faster

Good Job, KEV!



EPSS, SSVC Helping orgs prioritize and execute

Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization (Version 2.0)

Top rated CVEs from the last thirty days

We selected the 48 highest rated CVEs published in the last 30 days. They are shown here with the CVE and EPSS score.

CVE-2023-38205 83.2%	CVE-2022-28836 5.1%	CVE-2023-4714 2.1%	CVE-2023-4762 1.1%	CVE-2023-39361 0.6%	CVE-2021-39859 0.4%
CVE-2023-36761 57.1%	CVE-2023-37759 4.8%	CVE-2023-40150 2.0%	CVE-2023-4596 1.0%	CVE-2023-41012 0.5%	CVE-2019-16470 0.4%
CVE-2023-4863 31.9%	CVE-2023-41892 4.7%	CVE-2023-31069 1.9%	CVE-2023-42470 0.9%	CVE-2023-38204 0.5%	CVE-2023-2813 0.4%
CVE-2023-38831 23.9%	CVE-2023-26369 3.5%	CVE-2023-31067 1.6%	CVE-2023-34039 0.9%	CVE-2023-41330 0.5%	CVE-2021-21088 0.4%
CVE-2023-39026 6.6%	CVE-2023-20269 2.6%	CVE-2023-4613 1.3%	CVE-2023-38155 0.9%	CVE-2023-39631 0.5%	CVE-2022-28835 0.4%
CVE-2023-4634 5.7%	CVE-2022-34224 2.4%	CVE-2023-4614 1.3%	CVE-2023-31068 0.8%	CVE-2019-16471 0.5%	CVE-2023-41009 0.4%
CVE-2021-43018 5.1%	CVE-2022-34227 2.4%	CVE-2023-34723 1.3%	CVE-2023-36281 0.8%	CVE-2023-39141 0.5%	CVE-2023-41887 0.4%
CVE-2022-28834 5.1%	CVE-2023-42442 2.2%	CVE-2023-38146 1.1%	CVE-2023-39598 0.6%	CVE-2023-41179 0.5%	CVE-2020-18912 0.4%

There is Hope

We need to improve our attention precision - that is, ensure we as defenders are paying the right amount of attention to the right vulnerabilities.

We need to evaluate context when adding attention to a vulnerability.

Is it being exploited (maliciously?)

What is the EPSS Score?

What does it enable? (RCE, Info Leakage, etc)

How widespread is it?

“EPSS is more valuable when you don’t know if something is actively being exploited or not.”

Bonus Section!

You're Welcome?

R.I.P. cvetrends.com

As you might be aware, Twitter recently restricted its free API access, which has affected multiple communities that rely on Twitter's data, including cvetrends.com

I built cvetrends.com so the security community can monitor real-time, trending CVE mentions on Twitter for free.

Unfortunately, due to Twitter's recent API change, the site is currently unable to run.

I'm exploring what options, if any, would allow the site to keep running.

In the meantime, I'd like to say a big thank you for all your kind messages of support. I understand the impact of cvetrends being offline for all the people and organisations that use it.

It's a shame that these external factors are currently preventing cvetrends from being available to the community.

Simon

Where did you go?

Welcome to IOC.exchange!

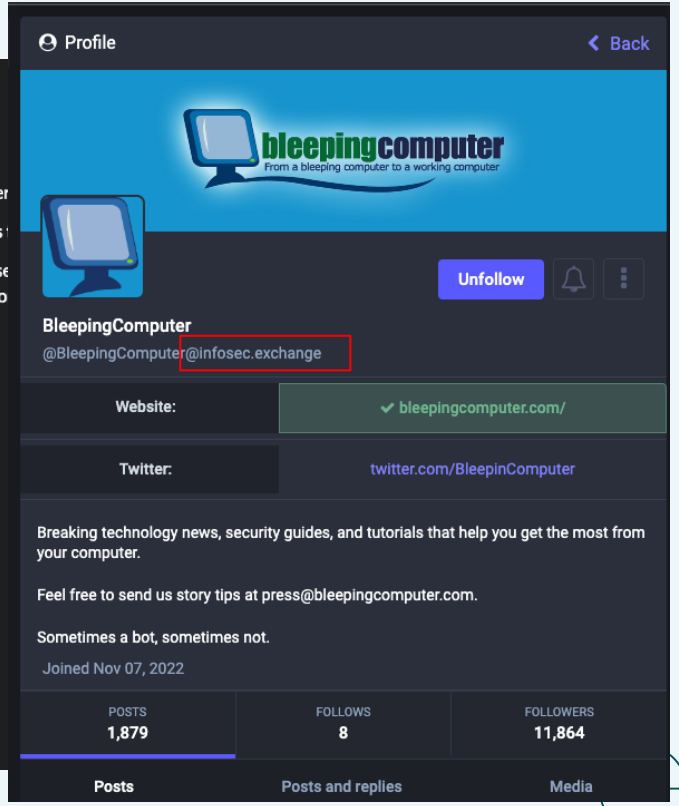
We are a community of InfoSec enthusiasts, professionals sharing not only cybersecurity info with each other

We welcome anyone, no matter your experience level. Our current user base ranges from infosec newbies

And while what is happening on our instance is great, the Fediverse as a whole has even more content and use
Million users spread over 5k+ instances). this guide has been written to make it easier for you to get started o

How to find more cyber folks on the Fediverse?

- Use Trunk to find people to follow for any topic - You can find cyber folks under InfoSec
- Check out user profiles on other infosec related instances:
  - hackers.town
  - freeradical.zone
  - infosec.exchange
  - chaos.social
  - social.privacytools.io
  - cybre.space
  - noc.social
- Search for infosec related public profiles across many instances:
  - instances.social
  - search.noc.social
- Check out who other people are following - Here is who seb is following.



And so… www.vulntrends.com

Top 10 CVE Strings (Last 30 Days):

cve	Count
CVE-2023-36845	9
CVE-2023-4863	9
CVE-2023-38146	5
CVE-2023-41179	4
CVE-2023-42793	4
CVE-2023-28434	3
CVE-2023-41992	2
CVE-2023-40477	2
CVE-2023-22513	2
CVE-2022-22265	2

CVE Trends for infosec.exchange