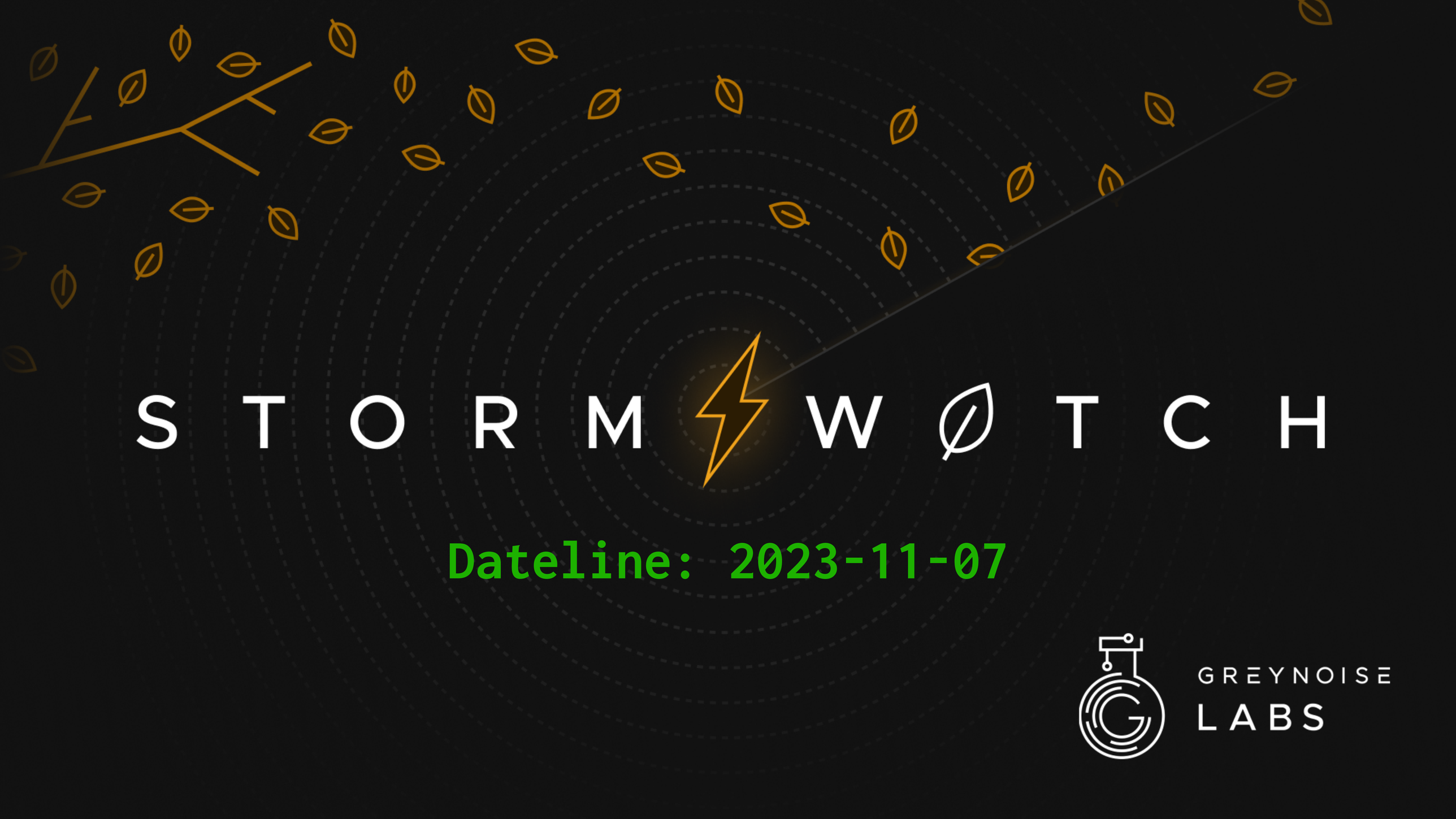

STORMWATCH
Dateline: 2023-11-07
GREYNOISE
LABS

Storm ⚡ Watch by GreyNoise Intelligence

GreyNoise Intelligence

TECHNOLOGY · UPDATED WEEKLY

GreyNoise Storm ⚡ Watch is a weekly podcast and livestream hosted by GreyNoise Intelligence (https://www.greynoise.io), a cybersecurity company that focuses on understanding internet noise. The show features hosts b MORE

https://pod.greynoise-storm.watch/

https://show.greynoise-storm.watch/

GREYNOISE LABS

STORM WATCH

~/cvecrowd$ _

https://cvecrowd.com/

About

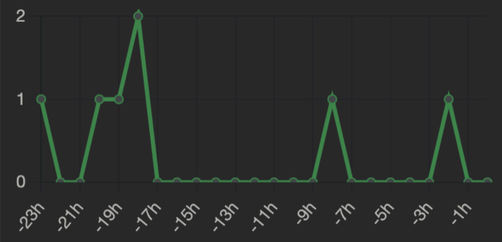
CVE-2023-22518

Atlassian Confluence Data Center

31 Oct 2023	07 Nov 2023
Published	Updated

CVSS v3.0 — CRITICAL (10.0)

7 Posts · 36 Interactions



CVE Info

All versions of Confluence Data Center and Server are affected by this unexploited vulnerability. This Improper Authorization vulnerability allows an unauthenticated attacker to reset Confluence and create a Confluence instance administrator account. Using this account, an attacker can then perform all administrative actions that are available to Confluence instance administrator leading to - but not limited to - full loss of confidentiality, integrity and availability. Atlassian Cloud sites are not affected by this vulnerability. If your Confluence site is accessed via an atlassian.net domain, it is hosted by Atlassian and is not vulnerable to this issue.

MITRE NVD

Fediverse

SANS Internet Storm Center - SANS.edu

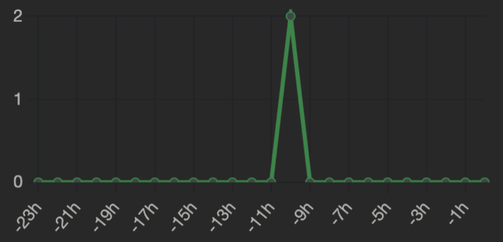
CVE-2022-26704

Apple macOS

26 May 2022	29 Jul 2022
Published	Updated

CVSS — Pending

2 Posts · 24 Interactions



CVE Info

A validation issue existed in the handling of symlinks and was addressed with improved validation of symlinks. This issue is fixed in macOS Monterey 12.4. An app may be able to gain elevated privileges.

MITRE NVD

Fediverse

Catalin Cimpanu
@campuscodi

Security researcher Gergely Kalman has published a technical write-up on BatSignal (CVE-2022-26704), an unprivileged user to root elevation of privilege vulnerability in macOS.
https://gergelykalman.com/no-CVE-batsignal-a-macos-lpe.html #infosec #cybersecurity #security #apple #macos #vulnerability

13 · 10 · 10 hours ago

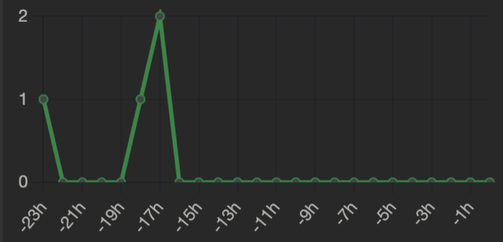
CVE-2023-46604

Apache Software Foundation ActiveMQ

27 Oct 2023	27 Oct 2023
Published	Updated

CVSS v3.1 — CRITICAL (10.0)

4 Posts · 11 Interactions



CVE Info

Apache ActiveMQ is vulnerable to Remote Code Execution.The vulnerability may allow a remote attacker with network access to a broker to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause the broker to instantiate any class on the classpath. Users are recommended to upgrade to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3, which fixes this issue.

MITRE NVD

Fediverse

Catalin Cimpanu
@campuscodi

Also:
-White Proxies proxy service linked to DDoS attacks on HU sites
-Unpatched Exchange vulnerabilities
-ActiveMQ bug (CVE-2023-46604) was a zero-

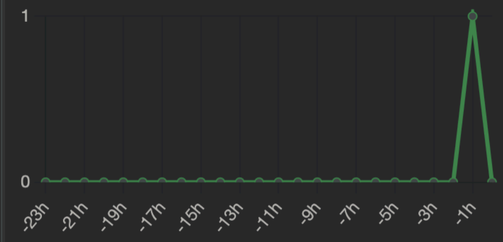
CVE-2023-42451

Pending

19 Sept 2023	Pending
Published	Updated

CVSS v3.1 — HIGH (7.5)

1 Post · 5 Interactions



CVE Info

Mastodon is a free, open-source social network server based on ActivityPub. Prior to versions 3.5.14, 4.0.10, 4.1.8, and 4.2.0-rc2, under certain circumstances, attackers can exploit a flaw in domain name normalization to spoof domains they do not own. Versions 3.5.14, 4.0.10, 4.1.8, and 4.2.0-rc2 contain a patch for this issue.

MITRE NVD

Fediverse

@chaos

And here we go for the 2nd blog post about a vulnerability in Mastodon. It details how HTTP signatures can be bypassed because of an innocuous bug, and how it can lead to the spoofing of Mastodon instances depending on their domain name. Don't worry, infosec.exchange wasn't vulnerable ;)


it's all good
GREYNOISE
LABS
STORM WØTCH

delivered by

https://www.legislation.gov.uk/uksi/2023/1007/contents/made

legislation.gov.uk

Cymraeg

Home | Browse Legislation | New Legislation | Coronavirus Legislation | Changes To Legislation | Search Legislation

Title: Search

Coordinated Vulnerability Disclosure!

The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023

UK Statutory Instruments ▸ 2023 No. 1007 ▸ Table of contents

Table of Contents

The following information must be published

- ⚡ Security reporting contact
- ⚡ ACK of receipt of security issue(s) report
- ⚡ Status updates for ^^
- ⚡ No £10 words or shenanigans in comms

Print Options

What Version

Latest available (Rev

Original (As made)

Opening Options

More Resources

inal format.

3. Security requirements for manufacturers

4. Deemed compliance with security requirements

5. Multiple manufacturers


BREAKING
NEWS

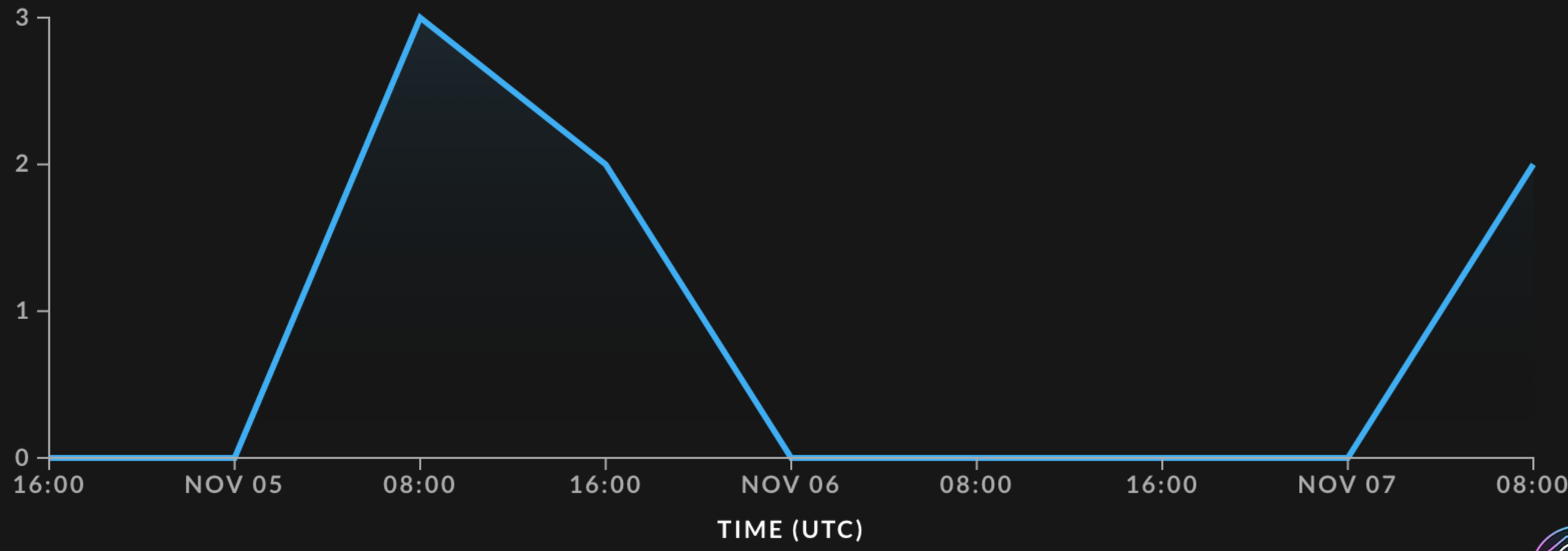
• 3 DAYS 10 DAYS 30 DAYS

November 04, 2023 - November 07, 2023

https://viz.greynoise.io/tag/atlassian-confluence-server-authentication-bypass-attempt?days=3

5

UNIQUE IPS OBSERVED BY GREYNOISE



atlassian-confluence-server-authentication-bypass-attempt

https://confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-server-1311473907.html

Updated CVSS score from 9.1 to 10, the summary of vulnerability, and added a threat detection section for suggested indicators of compromise

Customer report of an active exploitation added to heading.

Removed "or later" verbiage in fix versions table, only the listed fix versions are patched.

“We observed publicly posted critical information about the vulnerability which increases risk of exploitation.”

Added third option to "Apply temporary mitigations if unable to patch"

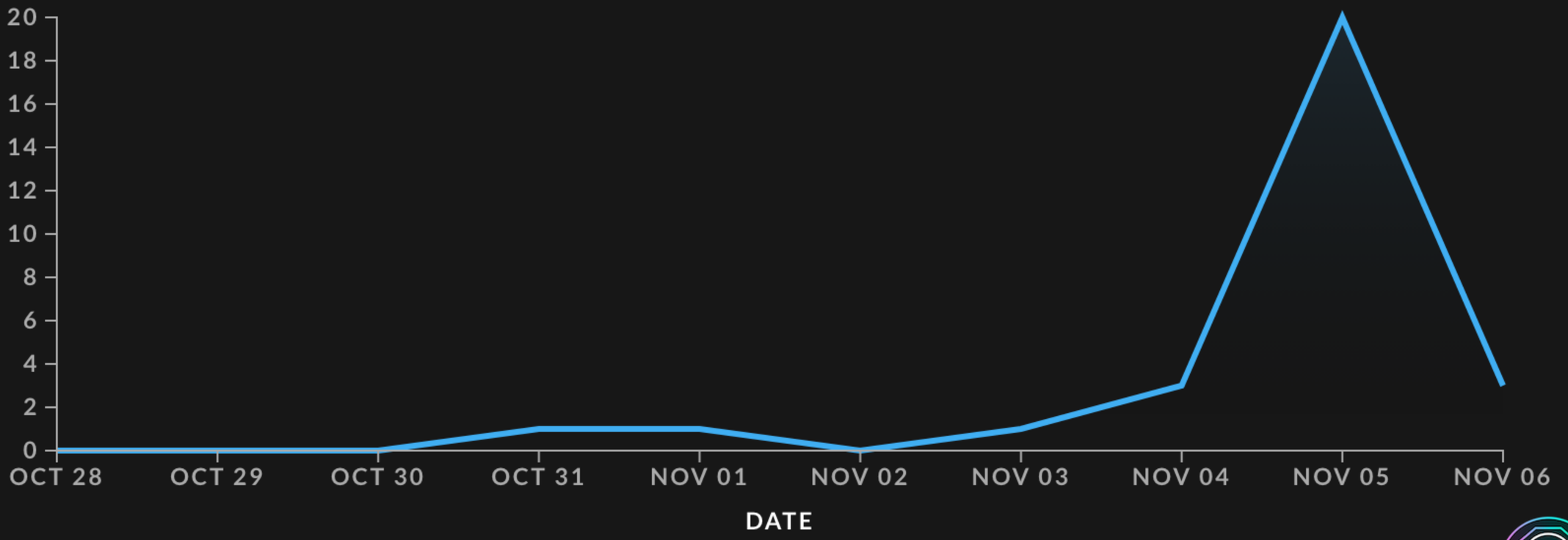
3 DAYS • 10 DAYS 30 DAYS

October 28, 2023 - November 07, 2023

https://viz.greynoise.io/tag/apache-activemq-rce-attempt?days=10

24

UNIQUE IPS OBSERVED BY GREYNOISE



apache-activemq-rce-attempt

3 DAYS 10 DAYS • 30 DAYS October 08, 2023 - November 07, 2023

https://viz.greynoise.io/tag/f5-big-ip-cve-2023-46747-rce-attempt?days=30

1

UNIQUE IPS OBSERVED BY GREYNOISE

f5-big-ip-cve-2023-46747-rce-attempt


BACK
TO THE FUTURE
OUTATIME

Verizon

+ 126 more

https://sec.okta.com/harfiles

GREYNOISE LABS

STORM WATCH

The most recent Okta breach affected 134 customers (<1% of Okta's customer base) & occurred between September 28, 2023, and October 17, 2023, when a threat actor gained unauthorized access to files inside Okta’s customer support system. Some of these files were HAR files that contained session tokens, which could be used for session hijacking attacks.

Prominent victims of the breach include Cloudflare, 1Password, and BeyondTrust. Other notable victims include Twillio and MailChimp.

Attempted attacks against entities like Cloudflare, T-Mobile, MetroPCS, Verizon, Slack, Twitter, CoinBase, Microsoft, Epic Games, Evernote, and Best Buy were observed, no successful breach of these organizations has been publicly reported.

Okta also experienced a 3rd-party breach (Rightway Healthcare) that resulted in the exposure of sensitive health information of almost 5,000 Okta employees but did not impact Okta services or customer data.

“During our investigation into suspicious use of this account, Okta Security identified that an employee had signed-in to their personal Google profile on the Chrome browser of their Okta-managed laptop,” Bradbury wrote. “The username and password of the service account had been saved into the employee’s personal Google account. The most likely avenue for exposure of this credential is the compromise of the employee’s personal Google account or personal device.”

https://arstechnica.com/information-technology/2023/11/no-okta-senior-management-not-an-errant-employee-caused-you-to-get-hacked/


NOW BACK TO OUR
REGULARLY SCHEDULED
PROGRAMMING

Security ID : **QSA-23-35**

Vulnerability in QTS, Multimedia Console, and Media Streaming add-on

Release date : November 4, 2023
CVE identifier : CVE-2023-23369
Affected products: QTS 5.1.x, 4.3.6, 4.3.4, 4.3.3, 4.2.x; Multimedia Console 2.1.x, 1.4.x; Media Streaming add-on 500.1.x, 500.0.x

An OS command injection vulnerability

Security ID : **QSA-23-31**

Vulnerability in QTS, QuTS hero, and QuTScloud

Release date : November 4, 2023
CVE identifier : CVE-2023-23368
Affected products: QTS 5.0.x, 4.5.x; QuTS hero h5.0.x, h4.5.x; QuTScloud c5.0.1

https://www.qnap.com/en-uk/security-advisory/qsa-23-35

Severity	Status
Critical	**Resolved**

QNAP

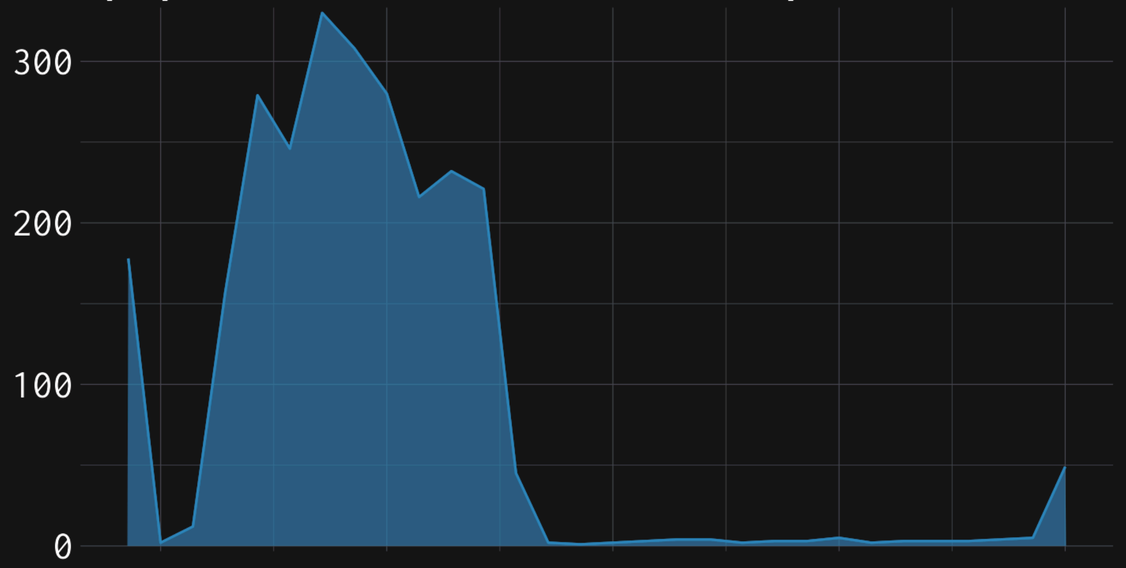
https://www.qnap.com/en-uk/security-advisory/qsa-23-31

https://www.qnap.com/en-uk/security-advisory/qsa-23-35

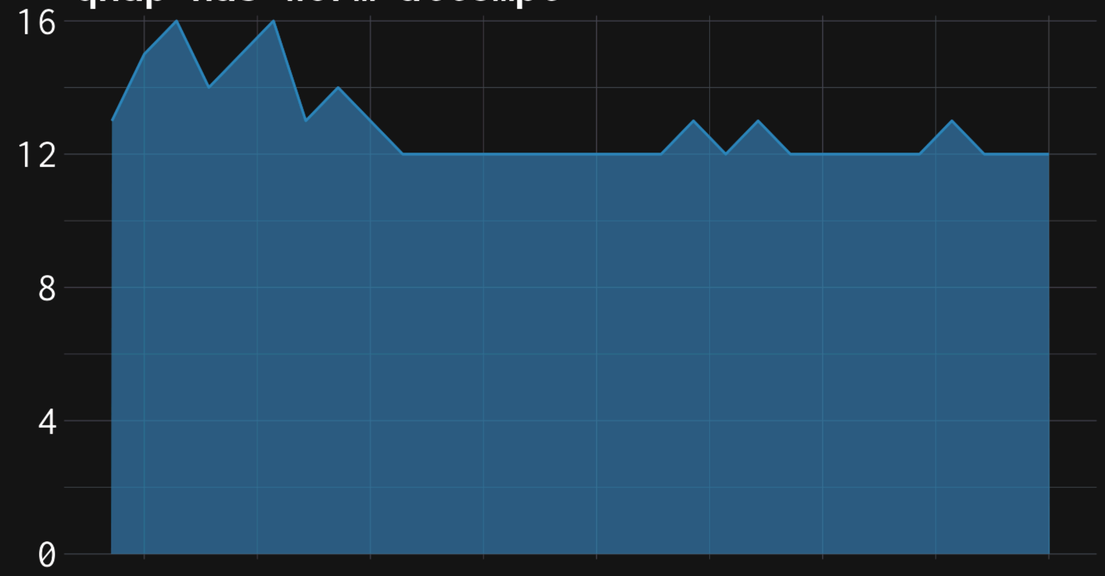
GREYNOISE LABS

STORM WATCH

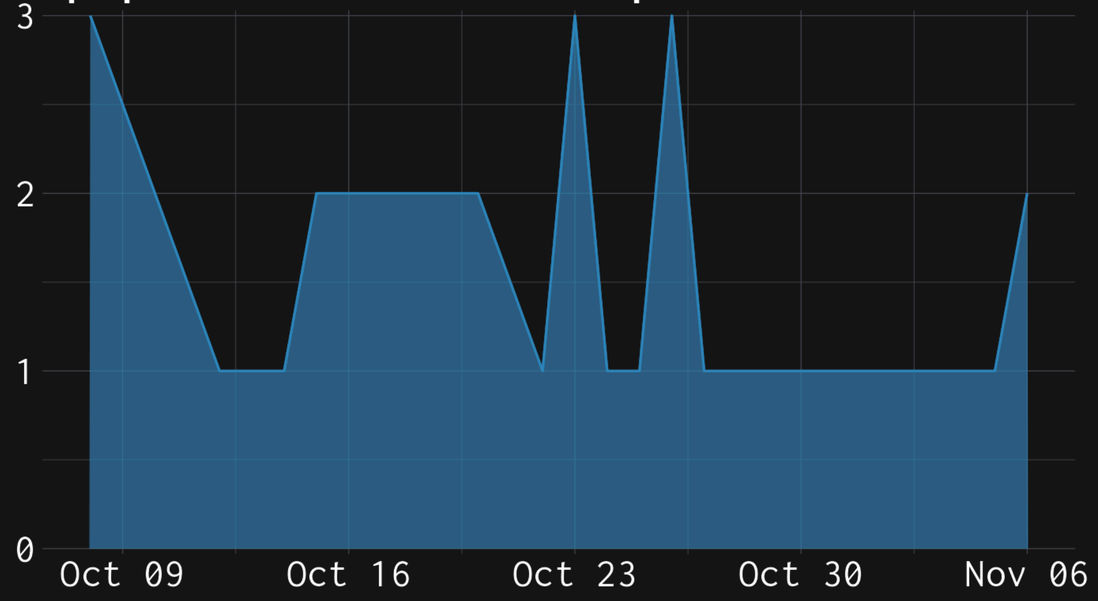
qnap-walter-ssh-backdoor-attempt



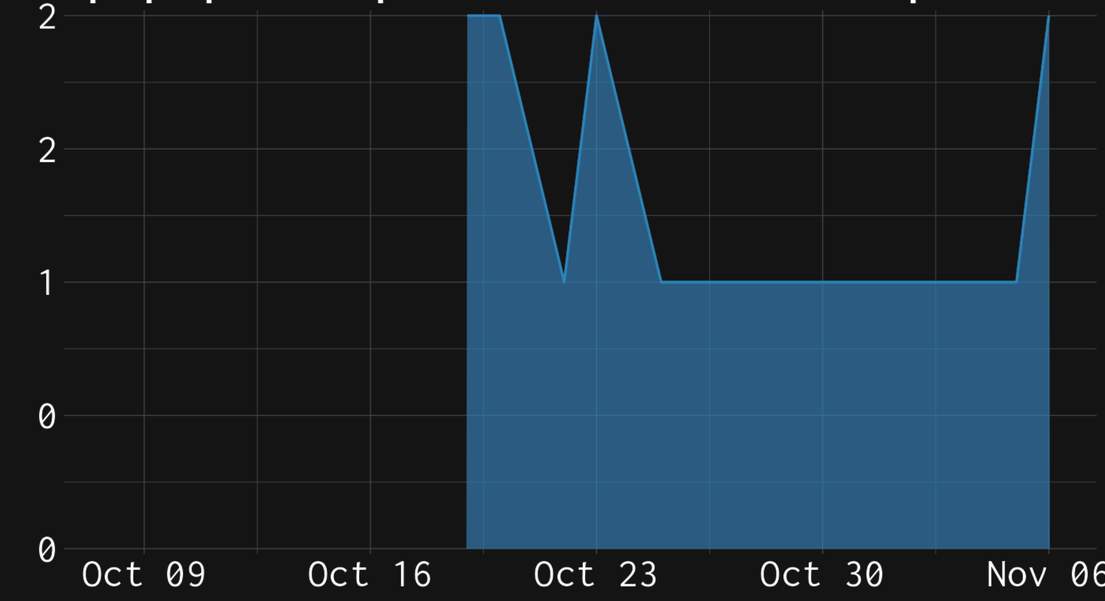
qnap-nas-worm-attempt



qnap-cve-2022-27593-attempt



qnap-qts-and-photo-station-lfi-attempt



https://blogs.cisco.com/security/the-myth-of-the-long-tail-vulnerability

October 30, 2023

Leave a Comment

Share

Security

The myth of the long-tail vulnerability

Ben Nahorney

Modern-day vulnerability management tends to follow a straightforward procedure. From a high level, this can be summed up in the following steps:

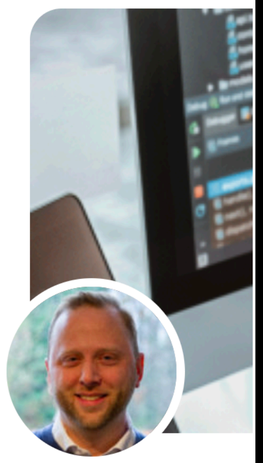
1. Identify the vulnerabilities in your environment

Cisco Blogs / Se

October 30, 2(

ave a Comment

Share



Modern-day

high level,

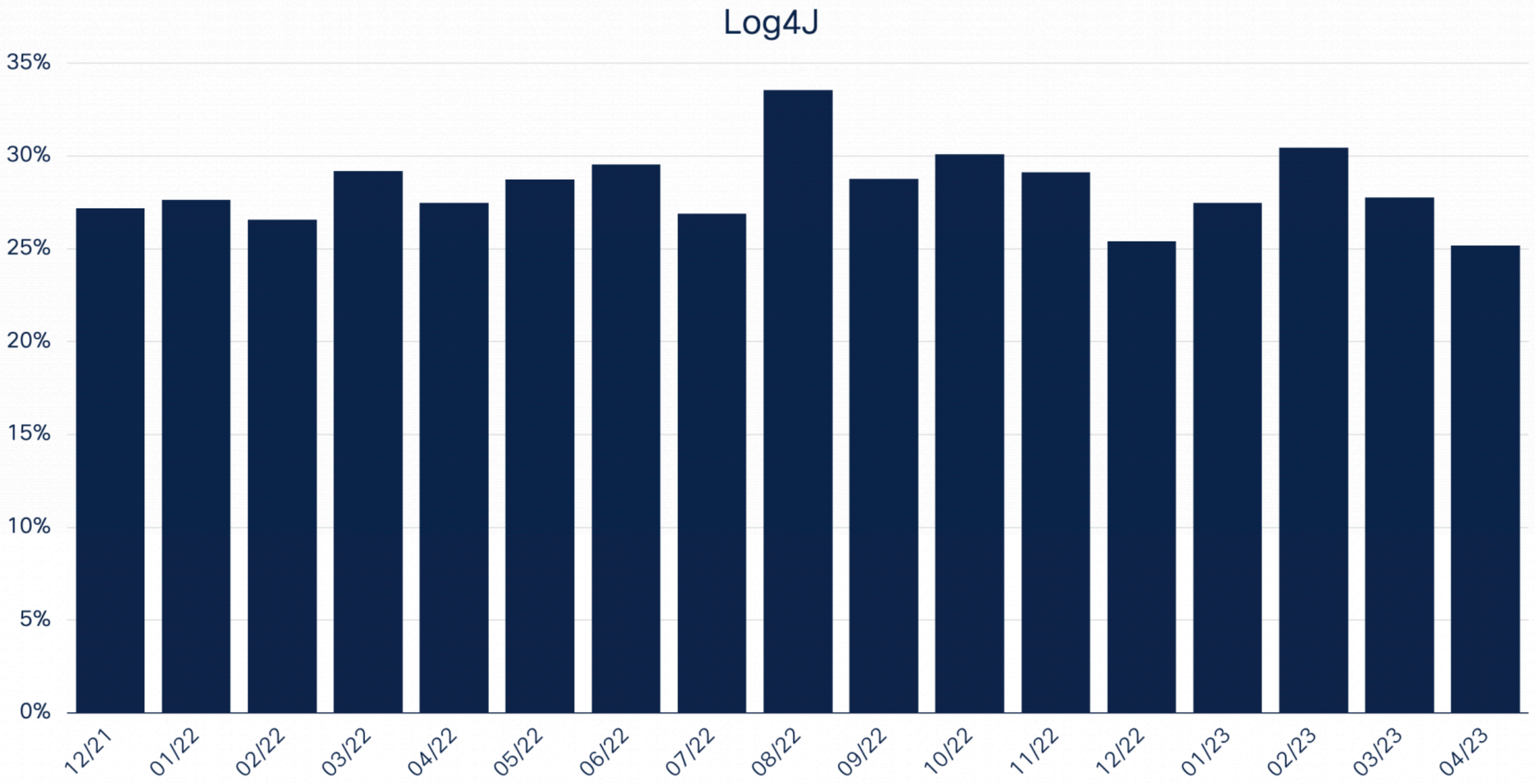
this can be s

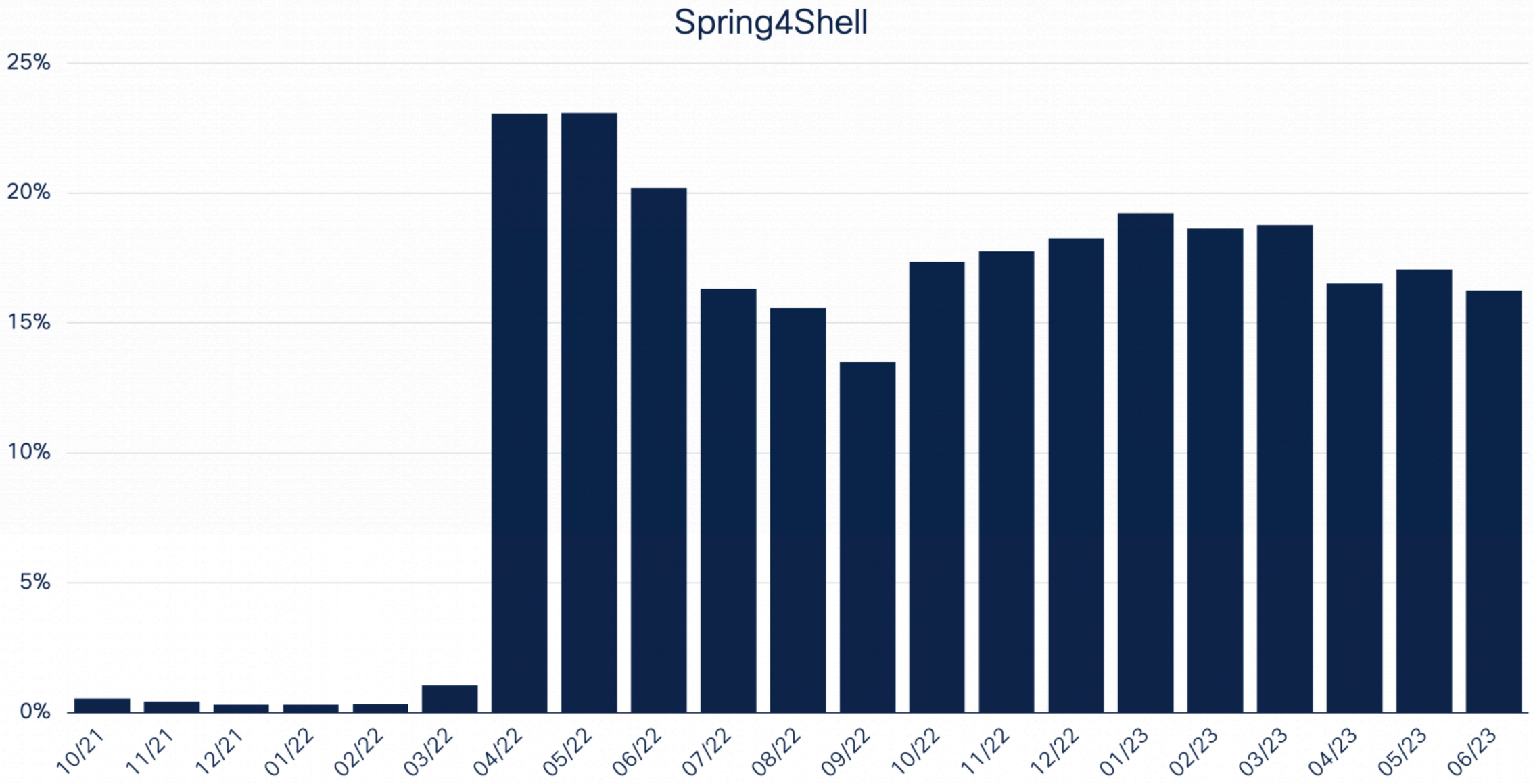
1. Identify the vulnerabilities in your environment

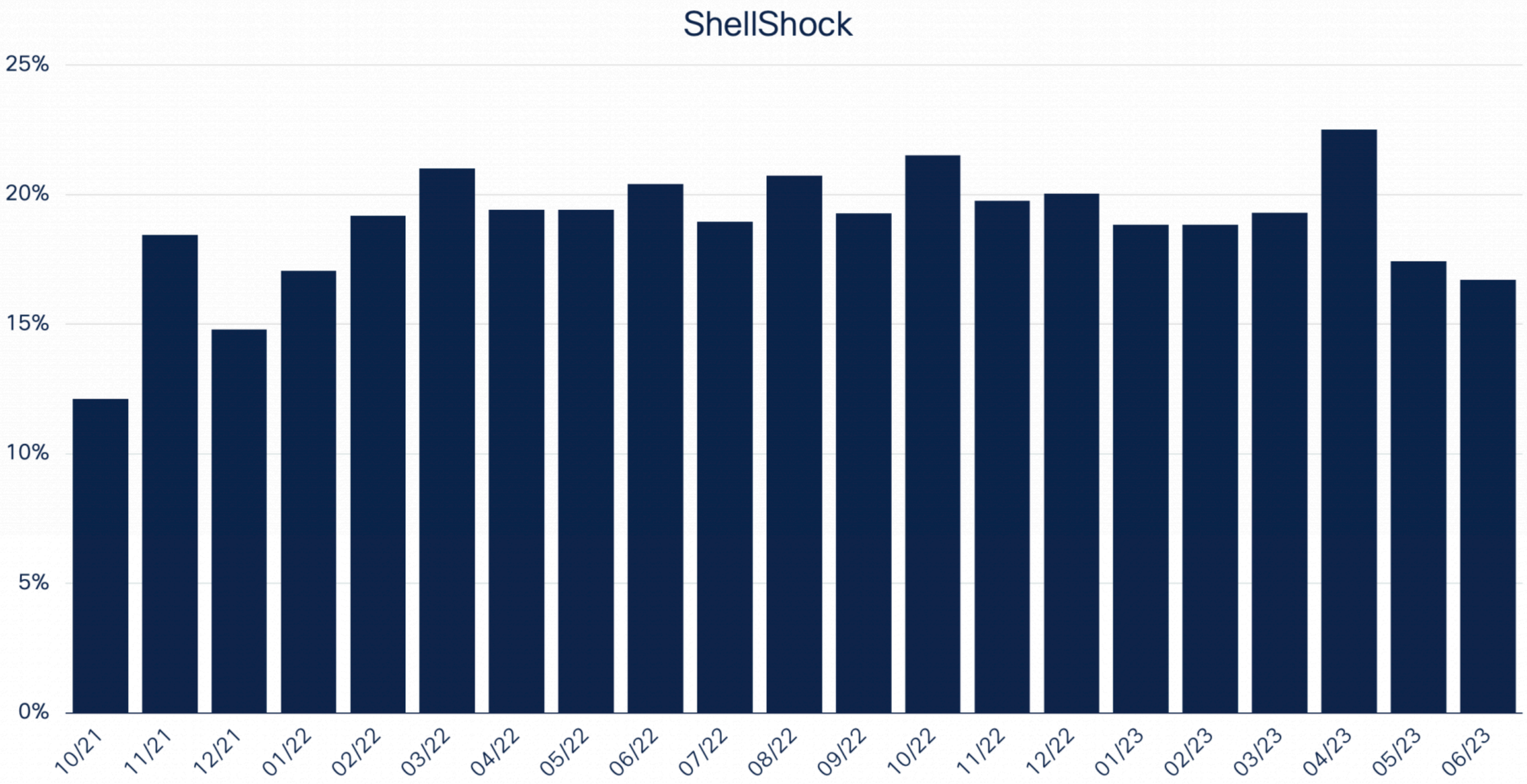
blogs.cisco.com/security

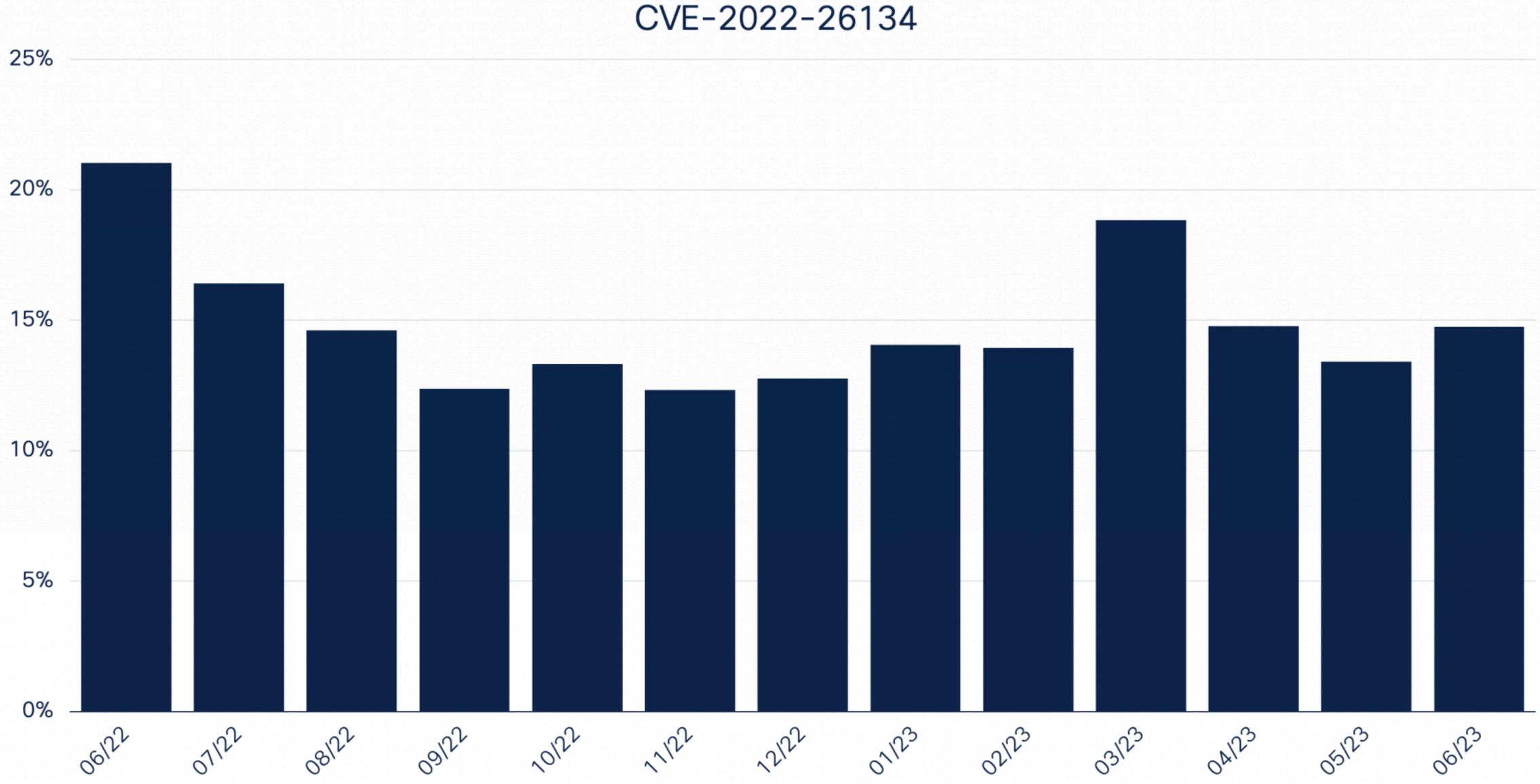
What emerges from looking at vulnerability alerts over time is that, while there is sometimes an initial spike in usage, they don't appear to decline to a negligible level. Instead, vulnerabilities stick around for years after their initial disclosure.

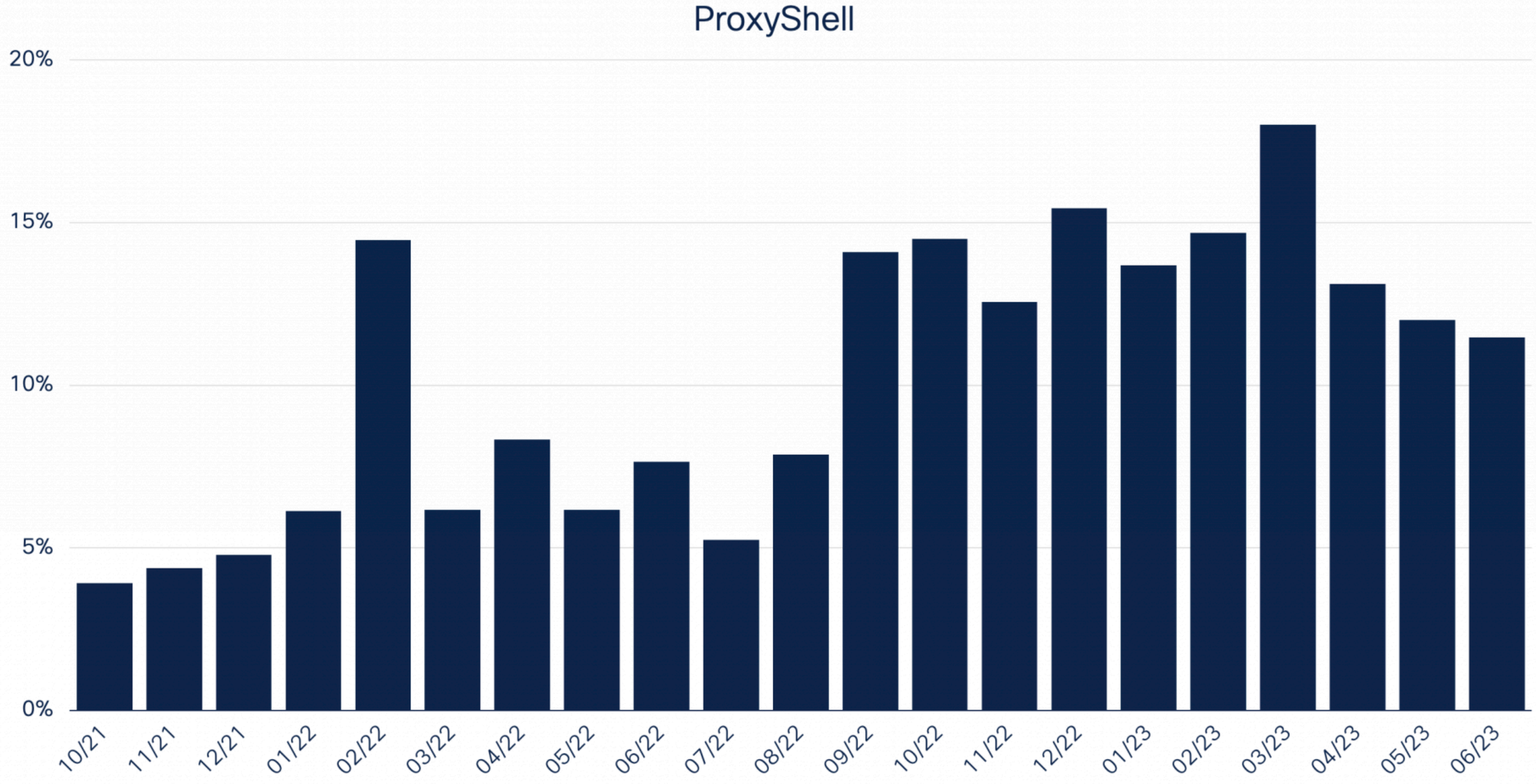
So why do old vulnerabilities remain in use? One reason is that many of these exploitation attempts are automated attacks. Bad actors routinely leverage scripts and applications that allow them to quickly run exploit code against a large swaths of IP addresses in the hopes of finding vulnerable machines.

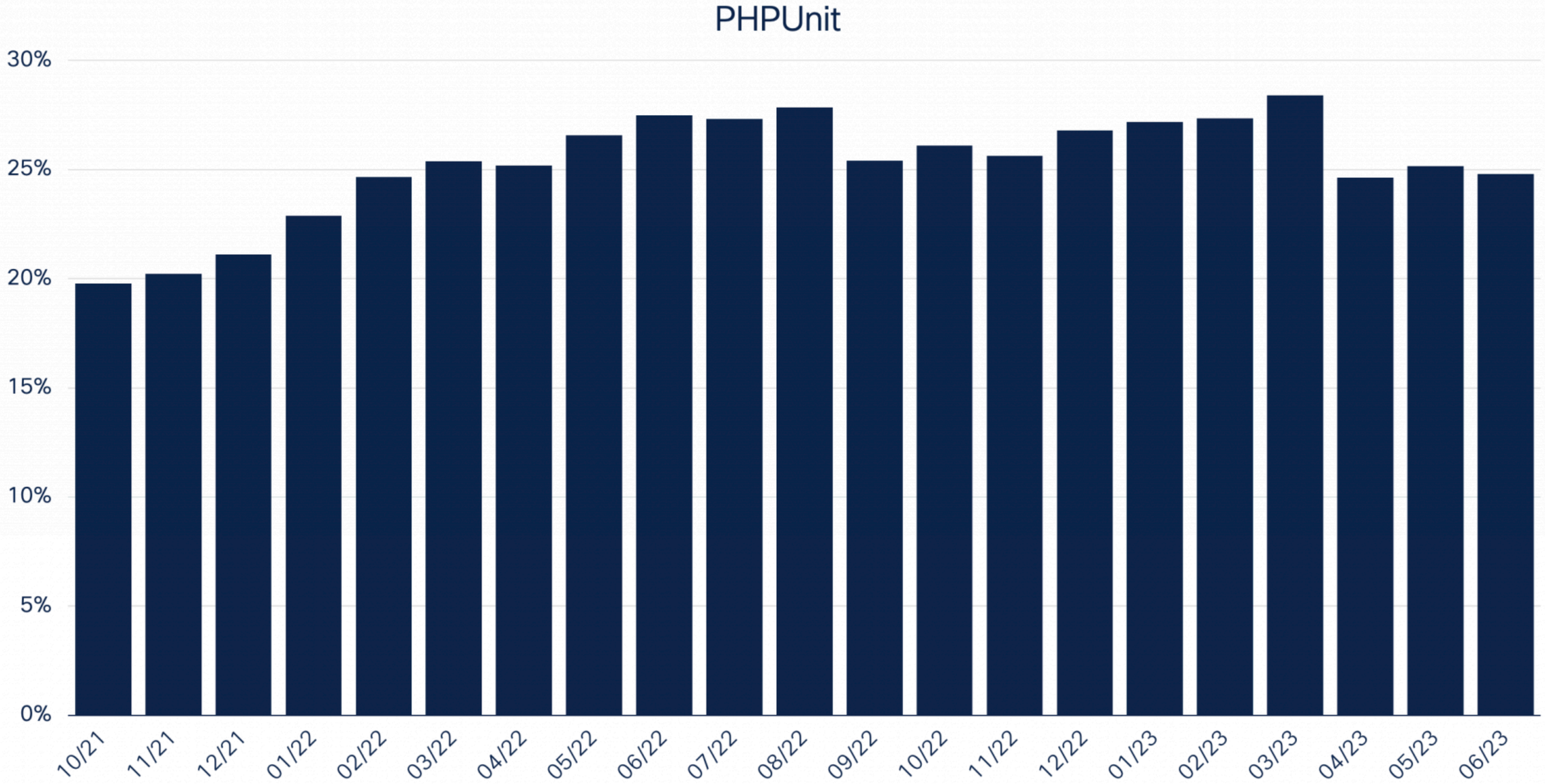












https://www.first.org/cvss/v4-0/index.html

FIRST Improving Security Together

About FIRST | Membership | Initiatives | Standards & Publications | Events | Education | Blog | Sign in

Common Vulnerability Scoring System (CVSS-SIG)

- Calculator
- Specification Document
- User Guide
- Examples
- Frequently Asked Questions
- **CVSS v4.0 Documentation & Resources**
  - CVSS v4.0 Calculator
  - CVSS v4.0 Specification Document
  - CVSS v4.0 User Guide
  - CVSS v4.0 Examples
  - CVSS v4.0 FAQ
- CVSS v3.1 Archive
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data Representations
- CVSS On-Line Training Course
- Identity & logo usage

Common Vulnerability Scoring System Version 4.0

CVSS version 4.0 is the next generation of the Common Vulnerability Scoring System standard.

Some of the changes incorporated into CVSS v4.0 include:

- Reinforce the concept that CVSS it not just the Base score
  - New nomenclature has been added to identify combinations of Base (CVSS-B), Base + Threat (CVSS-BT), Base + Environmental (CVSS-BE), and Base + Threat + Environmental (CVSS-BTE)
- Finer granularity through the addition of new Base metrics and values:
  - New Base metric: Attack Requirements (AT)
  - New Base metric values: User Interaction (UI): Passive (P) and Active (A)
- Enhanced disclosure of impact metrics:
  - Scope retired
  - Explicit assessment of impact to Vulnerable System (VC, VI, VA) and Subsequent Systems (SC, SI, SA)
- Temporal metric group renamed to Threat metric group
  - Threat metrics simplified and clarified
  - Remediation Level (RL) and Report Confidence (RC) retired
  - Exploit "Code" Maturity renamed to Exploit Maturity (E) with clearer values
- New Supplemental Metric Group to convey additional extrinsic attributes of a vulnerability that do not affect the final CVSS-BTE score
  - Safety (S)
  - Automatable (A)
  - Recovery (R)
  - Value Density (V)
  - Vulnerability Response Effort (RE)
  - Provider Urgency (U)
- Additional focus on OT/ICS/Safety
  - Consumer-assessed Safety (MSI:S, MSA:S)
  - Provider-assessed Safety through Safety (S) supplemental metric

More information about what's new in CVSS v4.0 is available in PDF format here .

CVSS COMMON VULNERABILITY SCORING SYSTEM

Chairs

- Dave Dugal
- Dale Rich

https://www.first.org/cvss/v4-0/index.html

FIRST Improving Security Together

About FIRST | Membership | Initiatives | Standards & Publications | Events | Education | Blog | Sign in

Common Vulnerability Scoring System (CVSS-SIG)

- Calculator
- Specification Document
- User Guide
- Examples
- Frequently Asked Questions
- **CVSS v4.0 Documentation & Resources**
  - CVSS v4.0 Calculator
  - CVSS v4.0 Specification Document
  - CVSS v4.0 User Guide
  - CVSS v4.0 Examples
  - CVSS v4.0 FAQ
- CVSS v3.1 Archive
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data Representations
- CVSS On-Line Training Course
- Identity & logo usage

Common Vulnerability Scoring System Version 4.0

Increased simplicity and clarity

CVSSv4 aims to simplify the scoring process and eliminate ambiguity by providing clearer guidance and definitions for metrics. This version fine-tunes the ideas of “Attack Complexity” and “Attack Requirements,” making the scoring process more understandable. These changes assist in more precise vulnerability assessment and ensure uniformity among various organizations.

CVSS COMMON VULNERABILITY SCORING SYSTEM

Chairs

- Dave Dugal
- Dale Rich

- Additional focus on OT/ICS/Safety
  - Consumer-assessed Safety (MSI:S, MSA:S)
  - Provider-assessed Safety through Safety (S) supplemental metric

More information about what's new in CVSS v4.0 is available in PDF format here .

https://www.first.org/cvss/v4-0/index.html

FIRST Improving Security Together

About FIRST | Membership | Initiatives | Standards & Publications | Events | Education | Blog | Sign in

Common Vulnerability Scoring System (CVSS-SIG)

- Calculator
- Specification Document
- User Guide
- Examples
- Frequently Asked Questions
- **CVSS v4.0 Documentation & Resources**
  - CVSS v4.0 Calculator
  - CVSS v4.0 Specification Document
  - CVSS v4.0 User Guide
  - CVSS v4.0 Examples
  - CVSS v4.0 FAQ
- CVSS v3.1 Archive
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data Representations
- CVSS On-Line Training Course
- Identity & logo usage

Common Vulnerability Scoring System Version 4.0

CVSS version 4.0 is the next generation of the Common Vulnerability Scoring System standard.

Some of the changes incorporated into CVSS v4.0 include:

- Reinforce
  - New nc (CVSS-E
- Finer gra
  - New Ba
  - New Ba
- Enhanced
  - Scope
  - Explicit
- Tempora
  - Threat
  - Remed
  - Exploit
- New Supp score
  - Safety (
  - Autom
  - Recove
  - Value Density (V)
  - Vulnerability Response Effort (RE)
  - Provider Urgency (U)
- Additional focus on OT/ICS/Safety
  - Consumer-assessed Safety (MSI:S, MSA:S)
  - Provider-assessed Safety through Safety (S) supplemental metric

nmental

/SS-BTE

More information about what's new in CVSS v4.0 is available in PDF format here .

CVSS COMMON VULNERABILITY SCORING SYSTEM

Chairs

- Dave Dugal
- Dale Rich

Renaming of Temporal Metrics to Threat Metrics

In CVSSv4, the "Temporal" metric from CVSSv3.1 has been renamed to "Threat Metrics". This change makes it much easier for end users to evaluate the severity of a vulnerability.

https://www.first.org/cvss/v4-0/index.html

FIRST Improving Security Together

About FIRST | Membership | Initiatives | Standards & Publications | Events | Education | Blog | Sign in

Common Vulnerability Scoring System (CVSS-SIG)

- Calculator
- Specification Document
- User Guide
- Examples
- Frequently Asked Questions
- **CVSS v4.0 Documentation & Resources**
  - CVSS v4.0 Calculator
  - CVSS v4.0 Specification Document
  - CVSS v4.0 User Guide
  - CVSS v4.0 Examples
  - CVSS v4.0 FAQ
- CVSS v3.1 Archive
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data Representations
- CVSS On-Line Training Course
- Identity & logo usage

Common Vulnerability Scoring System Version 4.0

CVSS version 4.0 is the next generation of the Common Vulnerability Scoring System standard.

Some of the changes incorporated into CVSS v4.0 include:

- Reinforce the concept that CVSS it not just the Base score
  - New nomenclature has been added to identify combinations of Base (CVSS-B), Base + Threat (CVSS-BT), Base + Environmental (CVSS-BE), and Base + Threat + Environmental (CVSS-BTE)
- Finer granularity through the addition of new Base metrics and values:

Retirement of Remediation Level (RL)

CVSSv4 also retired the "Remediation Level (RL)" metric from the previous version.

score
  - Safety (S)
  - Automatable (A)
  - Recovery (R)
  - Value Density (V)
  - Vulnerability Response Effort (RE)
  - Provider Urgency (U)
- Additional focus on OT/ICS/Safety
  - Consumer-assessed Safety (MSI:S, MSA:S)
  - Provider-assessed Safety through Safety (S) supplemental metric

More information about what's new in CVSS v4.0 is available in PDF format here .

CVSS COMMON VULNERABILITY SCORING SYSTEM

Chairs

- Dave Dugal
- Dale Rich

https://www.first.org/cvss/v4-0/index.html

FIRST Improving Security Together

About FIRST | Membership | Initiatives | Standards & Publications | Events | Education | Blog | Sign in

Common Vulnerability Scoring System (CVSS-SIG)

- Calculator
- Specification Document
- User Guide
- Examples
- Frequently Asked Questions
- **CVSS v4.0 Documentation & Resources**
  - CVSS v4.0 Calculator
  - CVSS v4.0 Specification Document
  - CVSS v4.0 User Guide
  - CVSS v4.0 Examples
  - CVSS v4.0 FAQ
- CVSS v3.1 Archive
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data Representations
- CVSS On-Line Training Course
- Identity & logo usage

Common Vulnerability Scoring System Version 4.0

CVSS version 4.0 is the next generation of the Common Vulnerability Scoring System standard.

Some of the changes incorporated into CVSS v4.0 include:

- Reinforce the concept that CVSS it not just the Base score
  - New nomenclature has been added to identify combinations of Base (CVSS-B), Base + Threat (CVSS-BT), Base + Environmental

Improved guidance for CVSS analysts

CVSSv4 provides improved guidance to CVSS analysts to produce consistent scores. It also provides guidance on scoring vulnerabilities in software libraries.

  - Automatable (A)
  - Recovery (R)
  - Value Density (V)
  - Vulnerability Response Effort (RE)
  - Provider Urgency (U)
- Additional focus on OT/ICS/Safety
  - Consumer-assessed Safety (MSI:S, MSA:S)
  - Provider-assessed Safety through Safety (S) supplemental metric

More information about what's new in CVSS v4.0 is available in PDF format here .

CVSS COMMON VULNERABILITY SCORING SYSTEM

Chairs

- Dave Dugal
- Dale Rich

https://www.first.org/cvss/v4-0/index.html

FIRST Improving Security Together

About FIRST | Membership | Initiatives | Standards & Publications | Events | Education | Blog | Sign in

Common Vulnerability Scoring System (CVSS-SIG)

- Calculator
- Specification Document
- User Guide
- Examples
- Frequently Asked Questions
- **CVSS v4.0 Documentation & Resources**
  - CVSS v4.0 Calculator
  - CVSS v4.0 Specification Document
  - CVSS v4.0 User Guide
  - CVSS v4.0 Examples
  - CVSS v4.0 FAQ
- CVSS v3.1 Archive
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data Representations
- CVSS On-Line Training Course
- Identity & logo usage

Common Vulnerability Scoring System Version 4.0

CVSS version 4.0 is the next generation of the Common Vulnerability Scoring System standard.

Some of the changes incorporated into CVSS v4.0 include:

- Reinforce the concept that CVSS it not just the Base score
  - New nomenclature has been added to identify combinations of Base (CVSS-B), Base + Threat (CVSS-BT), Base + Environmental

Support for multiple CVSS scores for the same vulnerability

CVSSv4 is designed to support multiple CVSS scores for the same vulnerability that affects multiple products, platforms, operating systems, etc.

  - Automatable (A)
  - Recovery (R)
  - Value Density (V)
  - Vulnerability Response Effort (RE)
  - Provider Urgency (U)
- Additional focus on OT/ICS/Safety
  - Consumer-assessed Safety (MSI:S, MSA:S)
  - Provider-assessed Safety through Safety (S) supplemental metric

More information about what's new in CVSS v4.0 is available in PDF format here .

CVSS COMMON VULNERABILITY SCORING SYSTEM

Chairs

- Dave Dugal
- Dale Rich

https://www.first.org/cvss/v4-0/index.html

FIRST Improving Security Together

About FIRST | Membership | Initiatives | Standards & Publications | Events | Education | Blog | Sign in

Common Vulnerability Scoring System (CVSS-SIG)

- Calculator
- Specification Document
- User Guide
- Examples
- Frequently Asked Questions
- **CVSS v4.0 Documentation & Resources**
  - CVSS v4.0 Calculator
  - CVSS v4.0 Specification Document
  - CVSS v4.0 User Guide
  - CVSS v4.0 Examples
  - CVSS v4.0 FAQ
- CVSS v3.1 Archive
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data Representations
- CVSS On-Line Training Course
- Identity & logo usage

Common Vulnerability Scoring System Version 4.0

CVSS version 4.0 is the next generation of the Common Vulnerability Scoring System standard.

Some of the changes incorporated into CVSS v4.0 include:

- Reinforce the concept that CVSS it not just the Base score
  - New nomenclature has been added to identify combinations of Base (CVSS-B), Base + Threat (CVSS-BT), Base + Environmental

Extension of the CVSS framework for other industry sectors

CVSSv4 provides guidance to extend the CVSS framework for other industry sectors such as privacy, automotive, etc.

  - Automatable (A)
  - Recovery (R)
  - Value Density (V)
  - Vulnerability Response Effort (RE)
  - Provider Urgency (U)
- Additional focus on OT/ICS/Safety
  - Consumer-assessed Safety (MSI:S, MSA:S)
  - Provider-assessed Safety through Safety (S) supplemental metric

More information about what's new in CVSS v4.0 is available in PDF format here .

CVSS COMMON VULNERABILITY SCORING SYSTEM

Chairs

- Dave Dugal
- Dale Rich

https://www.first.org/cvss/v4-0/index.html

FIRST Improving Security Together

About FIRST | Membership | Initiatives | Standards & Publications | Events | Education | Blog | Sign in

Common Vulnerability Scoring System (CVSS-SIG)

- Calculator
- Specification Document
- User Guide
- Examples
- Frequently Asked Questions
- **CVSS v4.0 Documentation & Resources**
  - CVSS v4.0 Calculator
  - CVSS v4.0 Specification Document
  - CVSS v4.0 User Guide
  - CVSS v4.0 Examples
  - CVSS v4.0 FAQ
- CVSS v3.1 Archive
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data Representations
- CVSS On-Line Training Course
- Identity & logo usage

Common Vulnerability Scoring System Version 4.0

Increased simplicity and clarity

CVSSv4 aims to simplify the scoring process and eliminate ambiguity by providing clearer guidance and definitions for metrics. This version fine-tunes the ideas of “Attack Complexity” and “Attack Requirements,” making the scoring process more understandable. These changes assist in more precise vulnerability assessment and ensure uniformity among various organizations.

CVSS COMMON VULNERABILITY SCORING SYSTEM

Chairs

- Dave Dugal
- Dale Rich

- Additional focus on OT/ICS/Safety
  - Consumer-assessed Safety (MSI:S, MSA:S)
  - Provider-assessed Safety through Safety (S) supplemental metric

More information about what's new in CVSS v4.0 is available in PDF format here .

https://digitalfrontlines.io/

CYBER OPERATIONS | MULTISTAKEHOLDER RESPONSES | FUTURE HYBRID WARS

Digital Front Lines

A sharpened focus on the risks of, and responses to, hybrid warfare.

GRE LABS

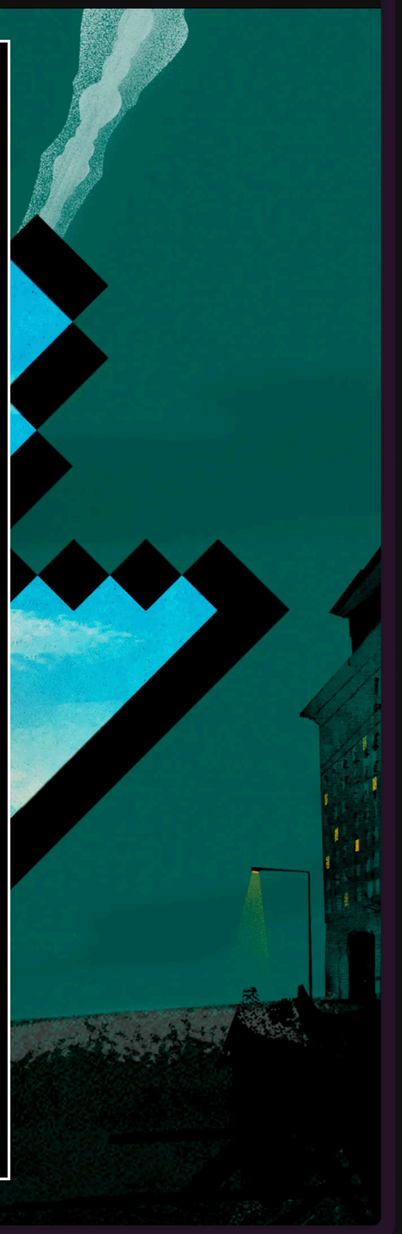
STORM WATCH

https://digitalfrontlines.io/

CYBER OPERATIONS | MULTISTAKEHOLDER RESPONSES | FUTURE HYBRID WARS

Digita
Front

A sharpened
responses to



In addition to deepening understanding of hybrid warfare, Digital Front Lines seeks to identify opportunities for collaboration across government, industry, and civil society to mitigate its destructive impacts. The contributions from experts in government, multilateral institutions, nongovernmental organizations, and the private sector along with research from FP Analytics underscore the need for sustained communication and coordination to adapt to the changing nature of warfare and effectively respond to the risks emerging from cyber operations.

https://www.wiz.io/blog/eight-questions-to-measure-vulnerability-remediation-pain

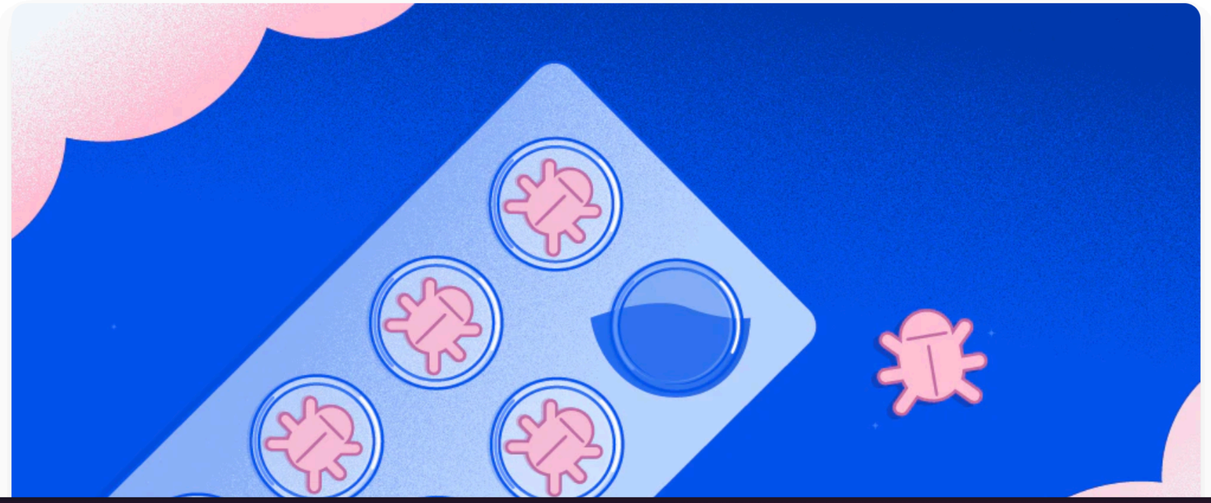
fyi

Eight questions to measure vulnerability remediation "pain"

What is it about certain vulnerabilities that makes them especially hard to deal with, and how can vendors make things easier for security teams?

Amitai Cohen
November 3, 2023

10 minutes read



censys

Threat Hunting Workshop & Happy Hour at CyberWeek

ShipGarten Brewing | 7581 Colshire Dr, McLean, VA
Wednesday, Nov 15 | 4-8 p.m.

4-6 pm: Threat Hunting Workshop -

Sit down with Censys threat hunters to learn tips and tricks on how to leverage the free Censys Search tool to identify and study threats across the Internet and within your own attack surface.

6-8 p.m: Happy Hour -

Enjoy happy hour drinks & appetizers on Censys! Network with security folks from around D.C. and mingle with a Special Guest who will be announced closer to the event!

SPECIAL GUEST

GREYNOISE

CENSYS PARTNER

carahsoft

Event Details

What to Expect

Spend a couple of hours enjoying craft beers & hot appetizers while you learn threat hunting tips and tricks from the pros at Censys:

- Find and investigate **C2 infrastructure** using fingerprints that Censys has created for Cobalt Strike, Dark Gate, and others
- **Live example of Malware**
- **Search labels**
  - With over 4,000 software and device labels, it's easier to find devices and services of interest
- **Exploring certificate data**
  - Useful for pivoting and identifying related infrastructure
  - Hunting for spoofed sites
- **Censys SDK/CLI for automation**
  - Subdomain enumeration command
- **Censys GPT**
  - CensysGPT harnesses the power of AI to enable users to express their search queries using natural language, significantly reducing the learning curve typically associated with mastering Censys Search Language.

RSVP Today and Join Us Nov 15 for...

Prizes for Threat Hunting Challenges, Free Swag, Craft Beer, Wine, & Full Bar, Heavy Appetizers, and MORE!

https://censys.com/cyberweek2023

GREYNOISE LABS

STORM WATCH

https://www.greynoise.io/blog/unveiling-the-deceptive-world-honeypots-vs-honeytokens

INSIGHTS

Unveiling the Deceptive World: Honeypots vs Honeytokens

Lacey Kasten | November 2, 2023

At GreyNoise, when we talk about honeypots, we sometimes get questions about honeytokens and how they differ. This may come from some of the great contributors to this space, making things like honeytokens widely available to experiment with (yay!). Setting up and deploying realistic and diversified honeypots is trickier, but there are still great contributors in closed and open-source projects.

Despite each's similar purpose of early threat detection, honeypots and honeytokens vastly differ in deployment, interaction, and scope. Let's delve into the various aspects contributing to the misunderstanding and clarify the distinctive features of each

Top Level GNQL Summary Stats

This notebook is updated hourly and provides summary statistics for five top-level GreyNoise GNQL queries. hit up labs@greynoise.io if you have questions or want to see more summaries.

Last data refresh: Tue, 07 Nov 2023 10:22:15 GMT

https://observablehq.com/@greynoise/top-level-gnql-summary-stats

Range: 1d

GNQL Query	▾Count	%
spoofable:true	261,022	55.14%
spoofable:false	225,346	44.86%

GNQL Query	▾Count	%
metadata.tor:false	485,774	99.98%
metadata.tor:true	594	0.02%

GNQL Query	▾Count	%
vpn:false	484,416	99.27%
vpn:true	1,952	0.73%

GNQL Query	▾Count	%
bot:false	485,534	99.89%
bot:true	834	0.11%

GNQL Query	▾Count	%
category:isp	309,506	67.12%
category:business	63,460	5.68%
category:mobile	59,062	14.46%
category:hosting	50,911	12.24%
category:education	1,243	0.50%

GNQL Query	▾Count	%
classification:unknown	386,075	82.82%
classification:malicious	94,973	16.91%
classification:benign	5,320	0.26%

Range: All

GNQL Query	▾Count	%
spoofable:true	3,765,537	55.14%
spoofable:false	3,063,448	44.86%

GNQL Query	▾Count	%
metadata.tor:false	6,827,548	99.98%
metadata.tor:true	1,437	0.02%

GNQL Query	▾Count	%
vpn:false	6,778,987	99.27%
vpn:true	49,998	0.73%

GNQL Query	▾Count	%
bot:false	6,821,781	99.89%
bot:true	7,204	0.11%

GNQL Query	▾Count	%
category:isp	4,480,916	67.12%
category:mobile	965,473	14.46%
category:hosting	816,802	12.24%
category:business	378,935	5.68%
category:education	33,568	0.50%

GNQL Query	▾Count	%
classification:unknown	5,655,999	82.82%
classification:malicious	1,154,931	16.91%
classification:benign	18,055	0.26%

- F5 BIG-IP CVE-2023-46747 RCE Attempt
- Beanshell Command Injection Attempt
- Apache ActiveMQ RCE Attempt
- Atlassian Confluence Server Authentication Bypass Attempt
- ads.txt Scanner

https://viz.greynoise.io/trends?view=recent

GREYNOISE LABS

STORM WØTCH

It Has Been

5

Days Since The
Last KEV Release

https://observablehq.com/@greynoise/greynoise-tags

GREYNOISE LABS

STORM WØTCH

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CVE-2023-46747
F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability

CVE-2023-46748
F5 BIG-IP Configuration Utility SQL Injection Vulnerability

CVE-2023-46604
Apache ActiveMQ Deserialization of Untrusted Data Vulnerability

https://www.cisa.gov/news-events/news/cisa-launches-critical-infrastructure-security-and-resilience-month-2023

PRESS RELEASE

CISA Launches Critical Infrastructure Security and Resilience Month 2023

The safety and security of our nation depends in large part on the resilience of our critical infrastructure. All critical infrastructure owners and operators must prepare for potential disruption—be able to respond with agility and to recover rapidly to minimize impacts to the services Americans rely on every hour of every day," said CISA Director Jen Easterly. "This Critical Infrastructure Security and Resilience Month, we are asking everyone to resolve to be more resilient by taking actionable steps to plan and exercise to withstand the impact of disruption.


Storm⚡Watch
GREYNOISE
LABS
STORM⚡WØTCH