

S T O R M ⚡ W ⚡ T C H

Dateline: 2023-11-14



GREYNOISE
LABS

S T O R M ⚡ W A T C H



Storm ⚡ Watch by GreyNoise Intelligence

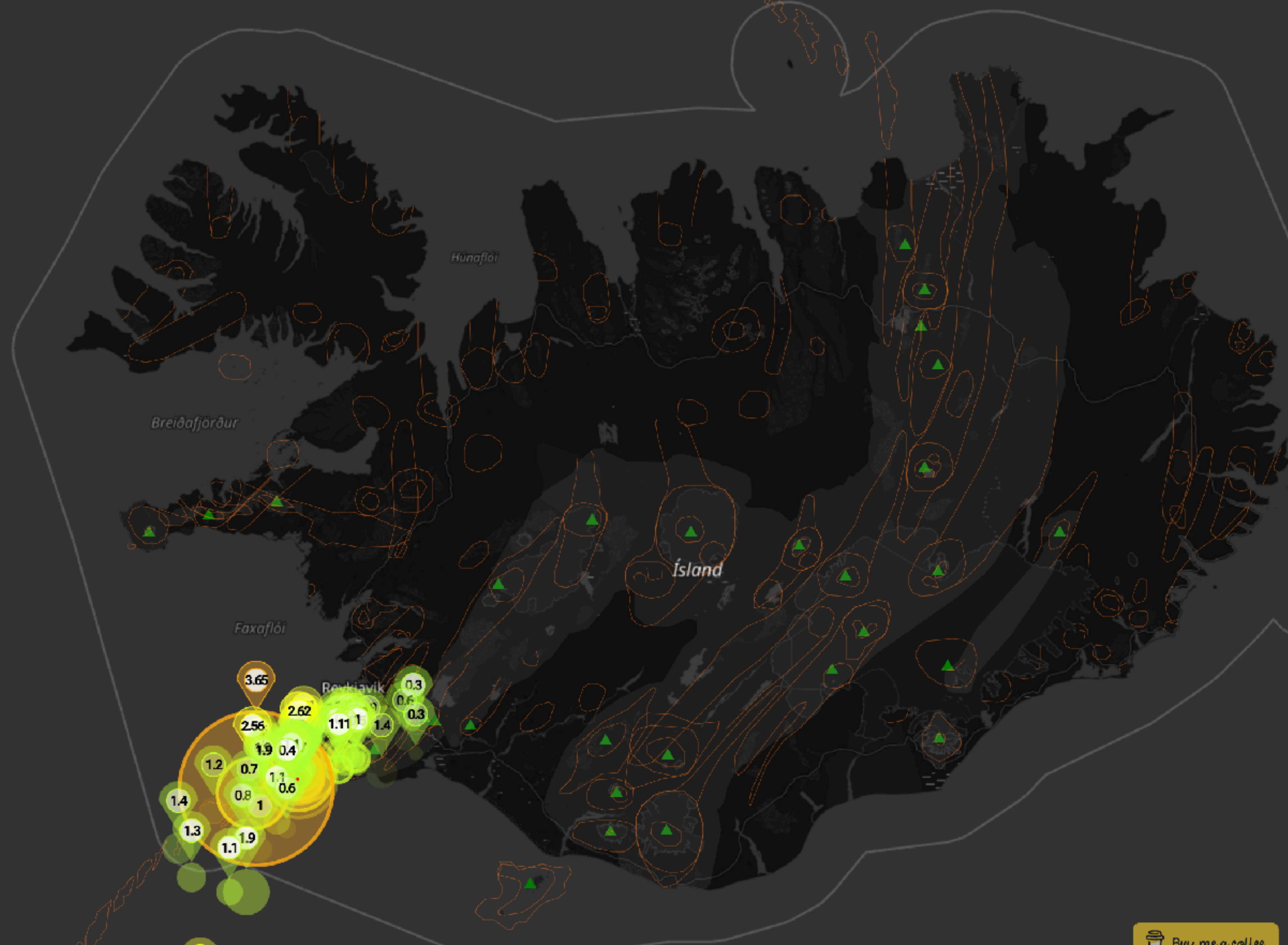
GreyNoise Intelligence

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/>

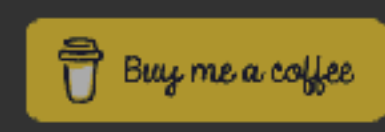


SKJÁLFTAR S.L. 6 KLST (152)

TÍMI	STÆRD	DÝPI	VIDV.SVÆÐI
10:20:11	1.2 aM	5.4 km	Svartsengi
10:15:06	1.1 aM	5.7 km	Reykjanes-skagi
10:13:06	0 aM	4.3 km	Krisuvík
10:08:40	1.2 aM	5.9 km	Svartsengi
10:02:19	0.2 aM	5.2 km	Svartsengi
09:59:54	0.7 aM	1.1 km	Svartsengi
09:59:25	1 aM	5.6 km	Svartsengi
09:56:22	0.9 aM	5.5 km	Svartsengi
09:55:28	0.1 aM	5.3 km	Svartsengi
09:54:05	1.1 aM	5.9 km	Svartsengi
09:45:59	1.1 aM	16.6 km	Ísland
09:45:24	0.6 aM	9.6 km	Brennisteinsfjöll
09:38:48	0.4 aM	5.6 km	Reykjanes-skagi
09:38:04	0.5 aM	4.5 km	Svartsengi
09:37:47	1.9 aM	1.1 km	Ísland
09:36:53	0 aM	5.2 km	Svartsengi
09:32:39	1.6 aM	5.0 km	Reykjanes
09:30:32	3.65 mlw	7.2 km	Reykjanes
09:30:15	0.6 aM	7.2 km	Svartsengi
09:30:12	1.11 mlw	2.8 km	Krisuvík
09:29:11	2.56 mlw	7.4 km	Reykjanes
09:28:17	0 aM	3.9 km	Svartsengi
09:26:38	1 aM	9.0 km	Krisuvík
09:26:12	1 aM	2.9 km	Brennisteinsfjöll
09:20:40	1.3 aM	4.1 km	Svartsengi
09:17:53	1.4 aM	5.0 km	Svartsengi
09:12:35	1.3 aM	5.6 km	Reykjanes-hryggur
09:08:14	1.28 mlw	3.9 km	Svartsengi
09:05:02	2.2 aM	9.7 km	Utan VVS - í hafi
09:02:27	2.48 mlw	5.6 km	Svartsengi
09:00:13	0.1 aM	2.1 km	Reykjanes-skagi
08:55:37	0.3 aM	5.2 km	Hengill

Svæði: Norður-Atlantshaf ▼ Stærð: > M0 ▼ Mesta dýpi: 25 km ▼ Tími: 6 klst ▼
 50 km

<https://vafri.is/quake/>



It's all good

IGP: Police arrest eight people in international syndicate which developed phishing templates to dupe victims [UPDATED]



By **Mohamed Basyir** - November 8, 2023 @ 2:52am



MOST POPULAR

LATEST

MOST READ

- 8m From lunch buddies, to life partners
- 9m Malaysia's palm oil output may taper off in coming months, weakening export demand expected too
- 15m KL Craft centre offers classes in batik making
- 19m Israeli army confirms identity of soldier held hostage by Hamas
- 20m #NSTviral: Supermarket customer calls out staff selling polybag oil to foreigners
- 23m Lexis bags nine accolades
- 26m 1962 Ferrari auctioned for US\$51.7mil in New York: Sotheby's



ACROSS NEW STRAITS TIMES



NST VIRAL 21 minutes ago
#NSTviral: Supermarket customer calls out staff selling polybag oil to foreigners



NATION 2 hours ago
Palestine-Israel conflict: Effects of boycott being felt



FOOTBALL Nov 13, 2023 @ 7:07am
A bold move by FAM



The Royal Malaysian Police have taken down the BulletProftLink phishing-as-a-service (PhaaS) platform, which provided over 300 phishing templates.

The operation began in 2015 but gained more attention in 2018 and had thousands of subscribers, some of whom paid for access to credential logs.

PhaaS platforms offer cybercriminals tools and resources for carrying out phishing attacks.

With the help of the Australian Federal Police and the FBI, the Malaysian police dismantled the operation and arrested eight individuals, including the suspected leader. They also seized cryptocurrency wallets, servers, computers, jewelry, vehicles, and payment cards.

The confiscated servers will be examined to identify users of the platform. Before being taken down, BulletProftLink had over 8,000 active subscribers with access to 327 phishing page templates.





**BREAKING
NEWS**



MOVEit Global Security Incident

Information for Maine Residents and Impacted Individuals

Maine encourages individuals to take steps to protect their personal information.

Related

[View the official press release here \(PDF\)](#)

Table of Contents

- ↓ [Overview](#)
- ↓ [What Happened?](#)
- ↓ [What Information Was Involved?](#)
- ↓ [Why Am I Hearing About This Now?](#)
- ↓ [What Did Maine Do to Respond to the Incident?](#)
- ↓ [How Do I Find Out if My Information Was Involved?](#)
- ↓ [Which State Departments/Agencies/Divisions Were Affected by the Incident?](#)
- ↓ [What Can I Do to Protect My Information?](#)
- ↓ [Contact/For More Information](#)

Overview

We are sharing information relating to a cyber incident that exploited a vulnerability in a widely used file transfer tool, MOVEit, which is owned by Progress Software. This event has had a global impact, affecting thousands of organizations, including certain agencies in



Maine government confirms cybercriminals exploited MOVEit vulnerability

Breach occurred between May 28 and 29, 2023

1.3 million individuals affected, including 534,194 Maine residents

Exposed data includes names, SSNs, birthdates, driver's license numbers, and taxpayer IDs

Some individuals had medical and health insurance information taken

Maine's Department of Health and Human Services most impacted





MOVEit Global Security Incident

Information for Maine Residents and Impacted Individuals

Maine encourages individuals to take steps to protect their personal information.

Related

[View the official press release here \(PDF\)](#)

2,388 organizations
67.5 – 72.4m individuals

- ↓ [How Do I Find Out if My Information Was Involved?](#)
- ↓ [Which State Departments/Agencies/Divisions Were Affected by the Incident?](#)
- ↓ [What Can I Do to Protect My Information?](#)
- ↓ [Contact/For More Information](#)

Overview

We are sharing information relating to a cyber incident that exploited a vulnerability in a widely used file transfer tool, MOVEit, which is owned by Progress Software. This event has had a global impact, affecting thousands of organizations, including certain agencies in



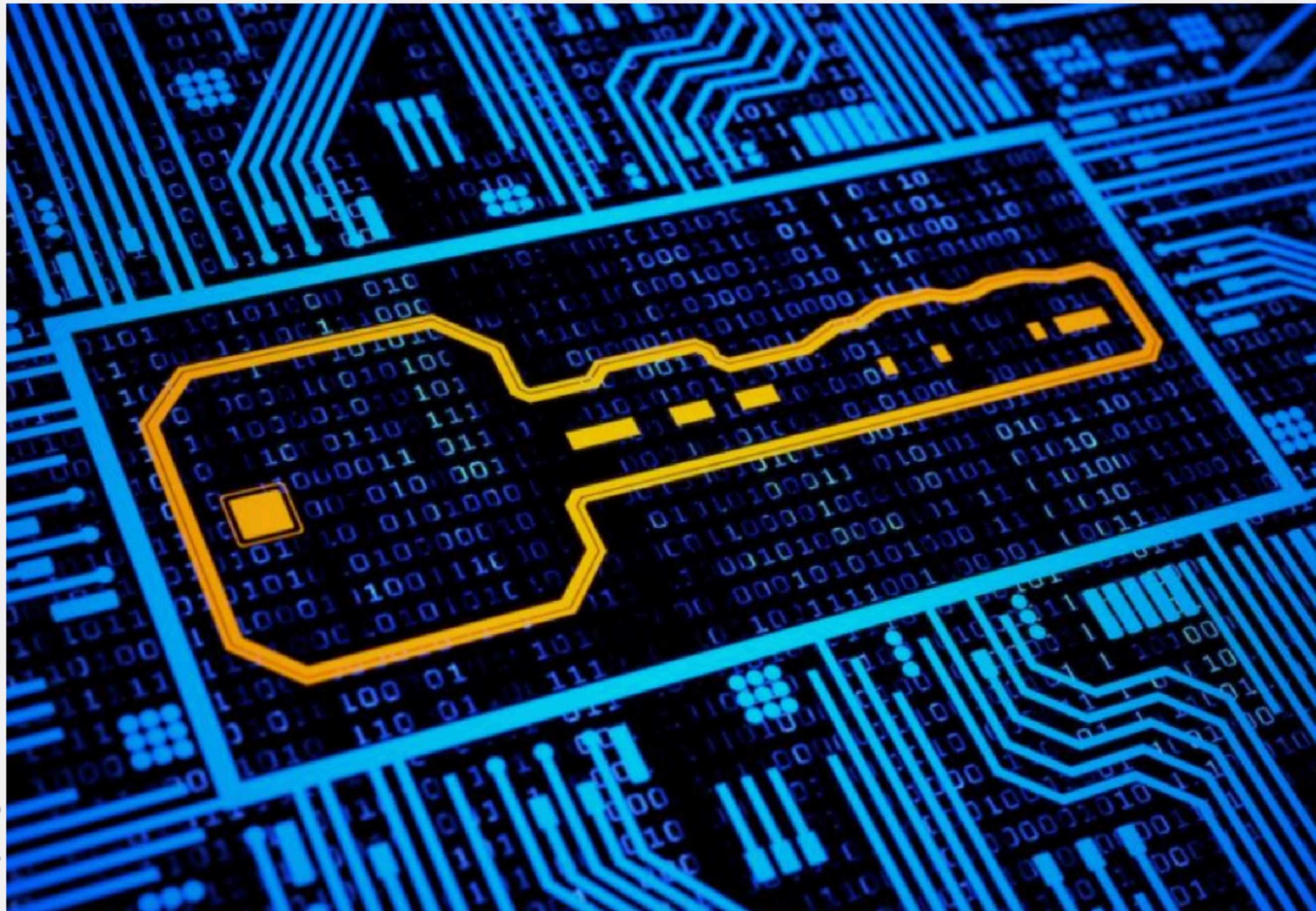
<https://arstechnica.com/security/2023/11/hackers-can-steal-ssh-cryptographic-keys-in-new-cutting-edge-attack/>

In a first, cryptographic keys protecting SSH connections stolen in new attack

An error as small as a single flipped memory bit is all it takes to expose a private key.

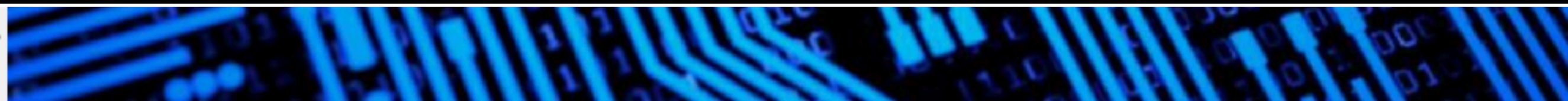
DAN GOODIN - 11/13/2023, 7:30 AM

<https://eprint.iacr.org/2023/1711.pdf>



Researchers have discovered that a significant number of cryptographic keys used to protect data in computer-to-server SSH traffic are vulnerable to compromise. The vulnerability occurs when errors happen during the signature generation process while establishing a connection. This affects RSA keys used in roughly a third of the SSH signatures examined, which translates to about 1 billion signatures out of 3.2 billion. Surprisingly, most SSH software, including OpenSSH, has deployed countermeasures to check for signature faults before sending them over the Internet.

Previously, it was believed that signature faults only exposed RSA keys used in TLS protocol encrypting web and email connections. However, SSH traffic was thought to be immune to such attacks. Since the release of TLS version 1.3 in 2018, the protocol has encrypted handshake messages, providing additional protection against key compromise. The researchers suggest that other protocols should include similar protection. While the majority of SSH connections are not affected, it is crucial to defend against these failures as one bad signature in an unprotected implementation can reveal the key.



In (rare) vulnerable targets, this allows you to recover the host's key, and thus impersonate a host. You can't compromise client credentials with this attack, since client credentials are exchanged after the (active) secure channel is established. If you can impersonate a host, as this attack would allow you to do, you could capture client password credentials, and you can drive a forwarded agent.

<https://news.ycombinator.com/item?id=38162996>

OpenSSH --- really, SSH servers on any Unix host you've been using in the last 20 years --- isn't vulnerable to this attack. The vulnerability is publishing a signature that is validly signed under RSA p and not under RSA q. Solution: just never do that; when you generate the signature, check it yourself before publishing. This is one of the better-known attacks on RSA, so this is a standard implementation countermeasure.

<https://news.ycombinator.com/item?id=38162996>

The things that are vulnerable are crappy middleboxes from Zyxel, Mocana, apparently a rare subset of Cisco devices, and whatever "SSH-2.0-SSHD" is (the authors don't know either).

<https://news.ycombinator.com/item?id=38162996>

<https://jadaptive.com/en/products/java-ssh-server>

<https://github.com/sshtools/j2ssh-maverick/blob/ce11ceaf0aa0b129b54327a6891973e1e34689f7/j2ssh-maverick/src/main/java/com/sshtools/ssh/SshConnector.java#L268>



**I WANT TO
BELIEVE**

NOISE

STORM



GREYNOISE TRENDS

↘ X SERVER CONNECTION ATTEMPT

TAG INTENT: Malicious
TAG CATEGORY: ↘ Activity

CVES:
CVE-1999-0526

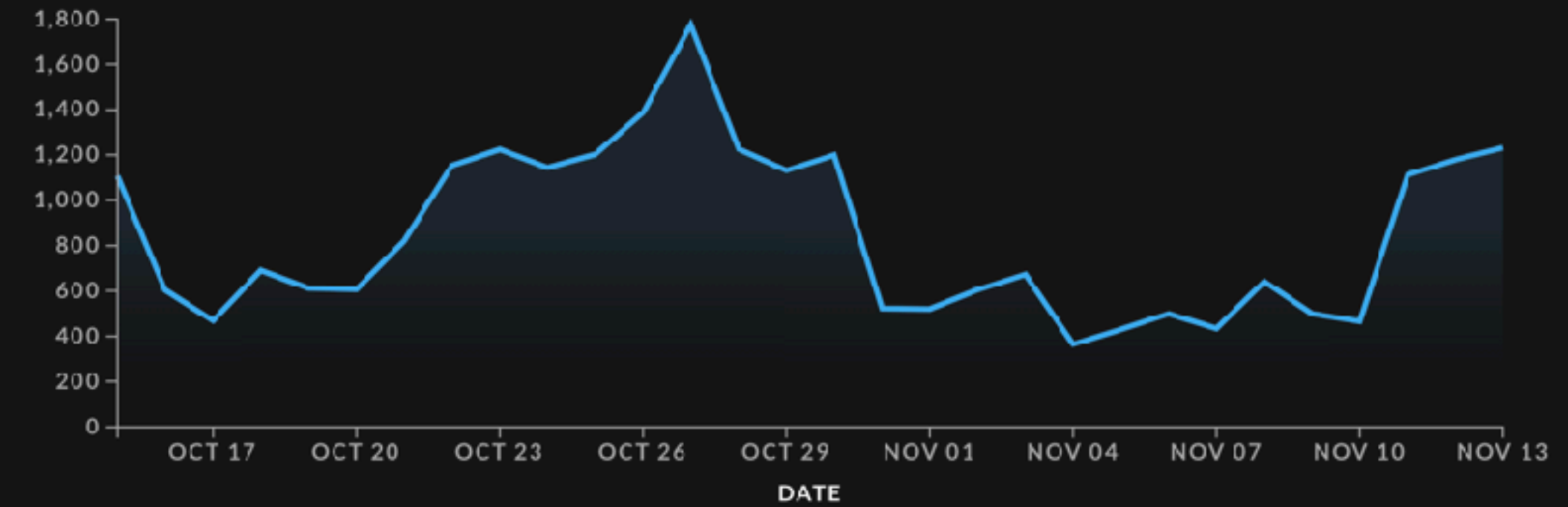
IP addresses with this tag have been observed scanning the Internet for X11 servers with access control disabled, which allows for unauthenticated connections.

3 DAYS 10 DAYS **• 30 DAYS**

October 15, 2023 - November 13, 2023

3,037

UNIQUE IPS OBSERVED BY GREYNOISE



**NOW BACK TO OUR
REGULARLY SCHEDULED
PROGRAMMING**



November 7, 2023

<https://www.sumologic.com/security-response-center/>

To Our Valued Customers:

At Sumo Logic, ensuring the security and reliability of our customers' digital experience is our top priority. We have always placed great emphasis on protecting our customers against threats, and we understand and deeply value the trust our customers place in us.

To that end, we are writing to notify you, as a precautionary measure, of a possible security incident within our platform.

WHAT HAPPENED:

On Friday, November 3rd, 2023, Sumo Logic discovered evidence of a potential security incident. The activity identified used a compromised credential to access a Sumo Logic AWS account. We have not at this time discovered any impacts to our networks or systems, and customer data has been and remains encrypted.

WHAT HAVE WE DONE:

Immediately upon detection we locked down the exposed infrastructure and rotated every potentially exposed credential for our infrastructure out of an abundance of caution. We are continuing to thoroughly investigate the origin and extent of this incident. We have identified the potentially exposed credentials and have added extra security measures to further protect our systems. This includes improved monitoring and fixing any possible gaps to prevent any similar events and we are continuing to monitor our logs to look for further signs of malicious activity. We have taken actions to stop the threat to our infrastructure and are advising customers





Sumo Logic detected unauthorized access to their AWS account using compromised credentials. However, there have been no impacts to their networks or systems, & customer data remains encrypted.

As a precautionary measure, they have locked down the exposed infrastructure & rotated potentially exposed credentials.

They are actively investigating the incident and have implemented additional security measures to prevent similar events.

They advise customers to rotate their credentials, including Sumo Logic installed collector credentials, third-party credentials stored with Sumo for data collection, and user passwords.

possible gaps to prevent any similar events and we are continuing to monitor our logs to look for further signs of malicious activity. We have taken actions to stop the threat to our infrastructure and are advising customers

https://www.bitdefender.com/blog/businessinsights/hive-ransomwares-offspring-hunters-international-takes-the-stage/

Hive Ransomware's Offspring: Hunters International Takes the Stage

 **Martin Zugec**
November 09, 2023



TOP POSTS



ENTERPRISE SECURITY • RANSOMWARE • THREAT RESEARCH

Hive Ransomware's Offspring: Hunters International Takes the Stage

November 09, 2023 • 📄



ENTERPRISE SECURITY • MANAGED DETECTION AND RESPONSE

Defending the Defenders: Understanding and Preventing Security Analyst Burnout

November 07, 2023 • 📄



ENTERPRISE SECURITY • ENDPOINT PROTECTION & MANAGEMENT • CYBERSECURITY AWARENESS

Unlocking Cyber Resilience: An SMBs 3-Step Game Plan

November 02, 2023 • 📄



ENTERPRISE SECURITY • BITDEFENDER THREAT DEBRIEF



THIS HIDDEN SITE HAS BEEN SEIZED



The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement effort against Hive Ransomware.



POLIZEI BADEN-WÜRTTEMBERG



https

stage/



<https://notcve.org/about.html>

— ABOUT THE !CVE PROGRAM —

The mission of the !CVE Program is to provide a common space for cybersecurity !vulnerabilities that are not acknowledged by vendors but still are serious security issues. In other words, these !vulnerabilities (read, *not vulnerabilities*) are security issues that would reduce the expected amount of work to be done by an attacker to successfully attack a target, but can also be fully fledged attacks on their own. We do believe !vulnerabilities should be identified, categorized and made known to the security community even when vendors refuse to acknowledge them or assign them a CVE.

According to MITRE's [CNA rules](#), vendors:

"[...] are left to their own discretion to determine whether something is a vulnerability."

This poses a clear conflict of interest, since the same vendor is the one deciding whether or not a CVE is assigned to their own product. As a result, this causes multiple security issues to not be assigned with a CVE even when MITRE agrees that one should be granted.

We see the !CVE Project as a great initiative to track and identify security issues that are not acknowledged by vendors but still are important for the security community.

© Copyright !CVE. All Rights Reserved



<https://notcve.org/about.html>

— ABOUT THE !CVE PROGRAM —

The mission of the !CVE Program is to provide a common space for cybersecurity !vulnerabilities that are not acknowledged by vendors but still are serious security issues. In other words, these !vulnerabilities (read, not vulnerabilities) are security issues that would reduce the expected amount of work to be done by an attacker to successfully attack a target, but can also be fully fledged attacks on their own. We do believe !vulnerabilities should be identified, categorized and made known to the security community even when vendors refuse to acknowledge them or assign them a CVE.

NotCVE-2023-0001 - Secure Boot Bypass in MSM8916/APQ8016 Mobile SoC

Date	CWE	Attack Type	Impact	CVSS
2023-05-23	CWE-1247:: Improper Protection Against Voltage and Clock Glitches	Physical	Confidentiality	7.6

Description

A physical attacker may leverage improper protection against voltage glitching in Qualcomm's Secure Boot implementation in chipsets MSM8916 and APQ8016 to execute arbitrary code in the device due to a badly secured hash value check.

Vendor	Product	Version	Package Name
Qualcomm	MSM8916/APQ8016/APQ8016E	1.0	-
Qualcomm	MSM8916/APQ8016/APQ8016E	Rev. D	-

Discoverer(s)/Credits

Cyber Intelligence S.L.

Common Attack Pattern Enumeration and Classification (CAPEC)



After the seizure of a ransomware group's infrastructure, a few common options emerge:

Continuing Operations: Some ransomware groups, even with disrupted infrastructure, persist by using backup resources or alternative communication channels to maintain their operations.

Rebranding and Evolution: Others opt for rebranding by changing their group's name, tactics, and techniques.


Disbandment: Some ransomware groups disband and disperse members to evade law enforcement scrutiny or to simply lay low.

Sale: In some cases, these operators, who own and develop the ransomware code and significant infrastructure, can decide to sell what's left of their criminal business to another ambitious group, passing on their tools and know-how to continue cybercriminal activities. This provides an opportunity for new actors to enter the ransomware landscape with a ready-made criminal enterprise.

TOOL TIME



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

 llaygoldman	Update README.md	dad2ed2 last week	🕒 7 commits
misc	Update ReadMe, requirements.txt		last week
.gitignore	Initial commit		last month
LICENSE	Update ReadMe, requirements.txt		2 weeks ago
README.md	Update README.md		last week
github_api_request_handler.py	initial commit		last month
requirements.txt	Update ReadMe, requirements.txt		2 weeks ago
scan_nvd.py	Update ReadMe, requirements.txt		last week

☰ README.md

CVE Half-Day Watcher [🔗](#)

CVE Half-Day Watcher is a security tool designed to highlight the risk of early exposure of Common Vulnerabilities and Exposures (CVEs) in the public domain. It leverages the National Vulnerability Database (NVD) API to identify recently published CVEs with GitHub references before an official patch is released. By doing so, CVE Half-Day Watcher aims to underscore the window of opportunity for attackers to "harvest" this information and develop exploits. This tool is a proof of concept, ready to be built upon and extended.

No description, website, or topics provided.

- 📖 Readme
- 📄 MIT license
- 📈 Activity
- ★ 62 stars
- 👁 3 watching
- 🍴 2 forks

Report repository

Releases

No releases published

Packages

No packages published

Contributors 2

-  llaygoldman

CVE Half-Day Watcher is a security tool designed to highlight the risk of early exposure of Common Vulnerabilities and Exposures (CVEs) in the public domain. It leverages the National Vulnerability Database (NVD) API to identify recently published CVEs with GitHub references before an official patch is released. By doing so, CVE Half-Day Watcher aims to underscore the window of opportunity for attackers to "harvest" this information and develop exploits. This tool is a proof of concept, ready to be built upon and extended.

exploits. This tool is a proof of concept, ready to be built upon and extended.

 Ilaygoldman

GitHub repository header for Aqua-Nautilus / CVE-Half-Day-Watcher. The repository is public and has 3 watchers, 2 forks, and 62 stars. It features a search bar, navigation links for Code, Issues, Pull requests, Actions, Projects, Security, and Insights. The repository name is CVE-Half-Day-Watcher, and it has 1 branch and 0 tags. A tooltip indicates the current URL has been copied.

A vulnerability that is known to the party or parties responsible for patching or fixing it. Alarmingly, this vulnerability is exposed on some public platforms such as GitHub commit/PR/issue, NVD, etc. A patch may have been created in the open-source, but the official release is not yet available.

CVE Half-Day Watcher is a security tool designed to highlight the risk of early exposure of Common Vulnerabilities and Exposures (CVEs) in the public domain. It leverages the National Vulnerability Database (NVD) API to identify recently published CVEs with GitHub references before an official patch is released. By doing so, CVE Half-Day Watcher aims to underscore the window of opportunity for attackers to "harvest" this information and develop exploits. This tool is a proof of concept, ready to be built upon and extended.

No packages published

Contributors 2

llygoldman

What is the risk? These kinds of vulnerabilities may be exposed on public platforms (such as NVD, GitHub, etc.), making it possible for attackers to harvest them, locate the vulnerable code, and even write an exploit. An example: imagine a case where there is an open issue on GitHub about “unwanted” behavior, and a commit that fixes the vulnerable code exists and refers to the issue, but the latest release on the GitHub project does not include the commit that resolves the issue.

recently published CVEs with GitHub references before an official patch is released. By doing so, CVE Half-Day Watcher aims to underscore the window of opportunity for attackers to "harvest" this information and develop exploits. This tool is a proof of concept, ready to be built upon and extended.

Contributors 2

llygoldman

CVE Half-Day Watcher scans the NVD for newly pushed CVEs and checks for any GitHub references such as commits, pull requests (PRs), or issues linked to these CVEs. It then verifies if the commit/PR has been included in a release on GitHub (currently for issue it skips this check). If a release including the fix is not available, it flags the CVE to indicate a possible "half-day" vulnerability scenario, where the vulnerability is known but not yet patched.

recently published CVEs with GitHub references before an official patch is released. By doing so, CVE Half-Day Watcher aims to underscore the window of opportunity for attackers to "harvest" this information and develop exploits. This tool is a proof of concept, ready to be built upon and extended.

Contributors 2

llygoldman

```
→ python3 scan_nvd.py --github_token "${GITHUB_TOKEN}" --days 10 --min_stars 5
https://services.nvd.nist.gov/rest/json/cves/2.0/?pubStartDate=2023-11-04T10:21:09&pubEndDate=2023-11-15T10:21:09&resultsPerPage=2000
found a possible half_day on CVE-2023-47249 with the reference: https://github.com/internationalcolorconsortium/demos/cmax/issues/54
found a possible half_day on CVE-2023-47271 with the reference: https://github.com/pkp/pkp-lib/issues/9464
found a possible half_day on CVE-2023-41378 with the reference: https://github.com/projectcalico/calico/pull/7908
found a possible half_day on CVE-2023-40660 with the reference: https://github.com/opensc/opensc/issues/2792#issuecomment-1674806651
found a possible half_day on CVE-2023-40661 with the reference: https://github.com/opensc/opensc/issues/2792#issuecomment-1674806651
found a possible half_day on CVE-2023-47004 with the reference: https://github.com/redisgraph/redisgraph/issues/3178
found a possible half_day on CVE-2023-2675 with the reference: https://github.com/linagora/twake/commit/0770da3b184b5d5e71fee8251a5847a04c7cb9bc
error in https://github.com/xwiki/xwiki-platform/commit/1dfb6804d4d412794cbe0098d4972b8ac263df0
found a possible half_day on CVE-2023-5900 with the reference: https://github.com/pkp/pkp-lib/commit/4d77a00be9050fac7eb8d2d1cbedcdaa1a5a803
found a possible half_day on CVE-2023-5901 with the reference: https://github.com/pkp/pkp-lib/commit/44d8bde60eb2575fd4087b76540aec9b49389e23
found a possible half_day on CVE-2023-5902 with the reference: https://github.com/pkp/pkp-lib/commit/2d04e770d2bbbdd899fdec382fbf2a1d4a4ffec8
found a possible half_day on CVE-2023-5903 with the reference: https://github.com/pkp/pkp-lib/commit/8b26ee404af3b11803a40e904f985f0a0b215a5c
found a possible half_day on CVE-2023-5904 with the reference: https://github.com/pkp/pkp-lib/commit/aa5c6acb634f460765facb2dc26df4b0d7424b
found a possible half_day on CVE-2023-46998 with the reference: https://github.com/bootboxjs/bootbox/issues/661
found a possible half_day on CVE-2023-33478 with the reference: https://github.com/remoteclinic/remoteclinic/issues/22
found a possible half_day on CVE-2023-33479 with the reference: https://github.com/remoteclinic/remoteclinic/issues/23
found a possible half_day on CVE-2023-33480 with the reference: https://github.com/remoteclinic/remoteclinic/issues/24
found a possible half_day on CVE-2023-33481 with the reference: https://github.com/remoteclinic/remoteclinic/issues/25
found a possible half_day on CVE-2023-5998 with the reference: https://github.com/gpac/gpac/commit/db74835944548fc3bdf03121b0e012373bdebb3e
found a possible half_day on CVE-2023-46001 with the reference: https://github.com/gpac/gpac/commit/e79b0cf7e72404750630bc01340e999f3940dbc4
found a possible half_day on CVE-2023-45857 with the reference: https://github.com/axios/axios/issues/6006
```





Shameless Self-Promotion

VULNERABILITIES

SLP Sliding Away With Reflection Amplification Thanks To CVE-2023-29552

Explore the high-severity vulnerability CVE-2023-29552 in the Service Location Protocol (SLP) that enables potential attackers to launch powerful Denial-of-Service (DoS) attacks. Learn about the potential impacts, the affected organizations, and the steps to mitigate this vulnerability. Discover how GreyNoise's new tag helps identify sources scanning for internet accessible endpoints exposing the SLP and how their customers can gain proactive protection.

boB Rudis | Nov 9, 2023



<https://www.greynoise.io/blog/slp-sliding-away-with-reflectionamplification-thanks-to-cve-2023-29552>



Analysis

Enrich and analyze IPs in bulk. Paste text containing IPs or upload a file.

Paste logs or other text containing IPs...

CLICK OR DRAG AND DROP TO UPLOAD FILES

Recommended file types: TXT, JSON, CSV, PCAP, PCAPNG



- 🏷️ favicon.ico Scanner
- 🏷️ Service Location Protocol Scanner
- 🏷️ phpDocumentor RCE Check

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

3 DAYS

• 10 DAYS

30 DAYS

November 04, 2023 - November 13, 2023

2,997

UNIQUE IPS OBSERVED BY GREYNOISE



LABS

STORM WATCH

3 DAYS

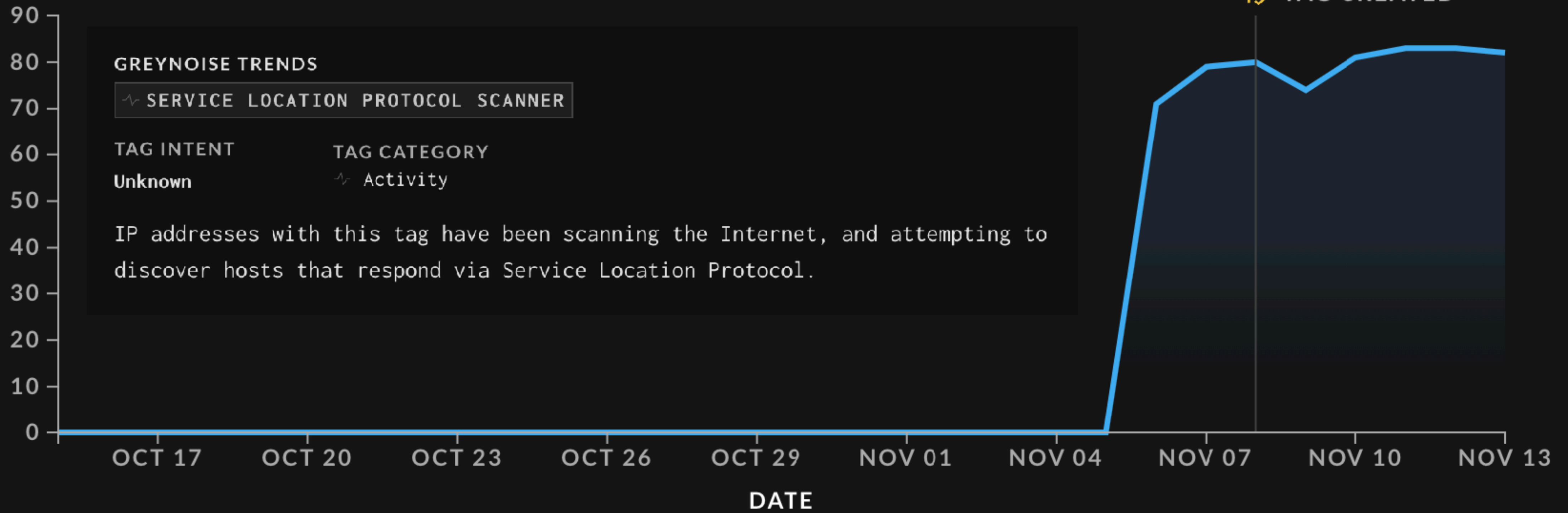
10 DAYS

• 30 DAYS

October 15, 2023 - November 13, 2023

98

UNIQUE IPS OBSERVED BY GREYNOISE



GREYNOISE TRENDS

~ SERVICE LOCATION PROTOCOL SCANNER

TAG INTENT

Unknown

TAG CATEGORY

~ Activity

IP addresses with this tag have been scanning the Internet, and attempting to discover hosts that respond via Service Location Protocol.

+ TAG CREATED



LABS

STORM WATCH

**WE NEED
TO TALK
ABOUT
KEY**

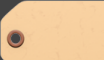







It Has Been

1

Days Since The
Last KEV Release

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

- ✘  CVE-2023-22518: Atlassian Confluence Data Center and Server Improper Authorization Vulnerability
- ✘ CVE-2023-29552: Service Location Protocol (SLP) Denial-of-Service Vulnerability
- ✘  CVE-2023-47246: SysAid Server Path Traversal Vulnerability
- ✘  CVE-2023-36844: Juniper Junos OS EX Series PHP External Variable Modification Vulnerability
- ✘  CVE-2023-36845: Juniper Junos OS EX Series and SRX Series PHP External Variable Modification Vulnerability
- ✘  CVE-2023-36846: Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability
- ✘  CVE-2023-36847: Juniper Junos OS EX Series Missing Authentication for Critical Function Vulnerability
- ✘ CVE-2023-36851: Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability

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



GREYNOISE TRENDS

ATLASSIAN CONFLUENCE SERVER AUTHENTICATION BYPASS ATTEMPT

TAG INTENT

Malicious

TAG CATEGORY

Activity

CVES:

CVE-2023-22518

IP addresses with this tag have been observed attempting to exploit CVE-2023-22518, an authentication bypass vulnerability in Atlassian Confluence Server.

3 DAYS

10 DAYS

• 30 DAYS

October 15, 2023 - November 13, 2023

10

UNIQUE IPS OBSERVED BY GREYNOISE



GREYNOISE TRENDS

JUNIPER JUNOS OS ENVIRONMENT VARIABLE INJECTION ATTEMPT

TAG INTENT

Malicious

TAG CATEGORY

Activity

CVES:

CVE-2023-36844

CVE-2023-36845

IP addresses with this tag have been observed attempting to exploit CVE-2023-36844 or CVE-2023-36845, an environment variable injection vulnerability in Juniper Junos OS SRX and EX Series.

3 DAYS

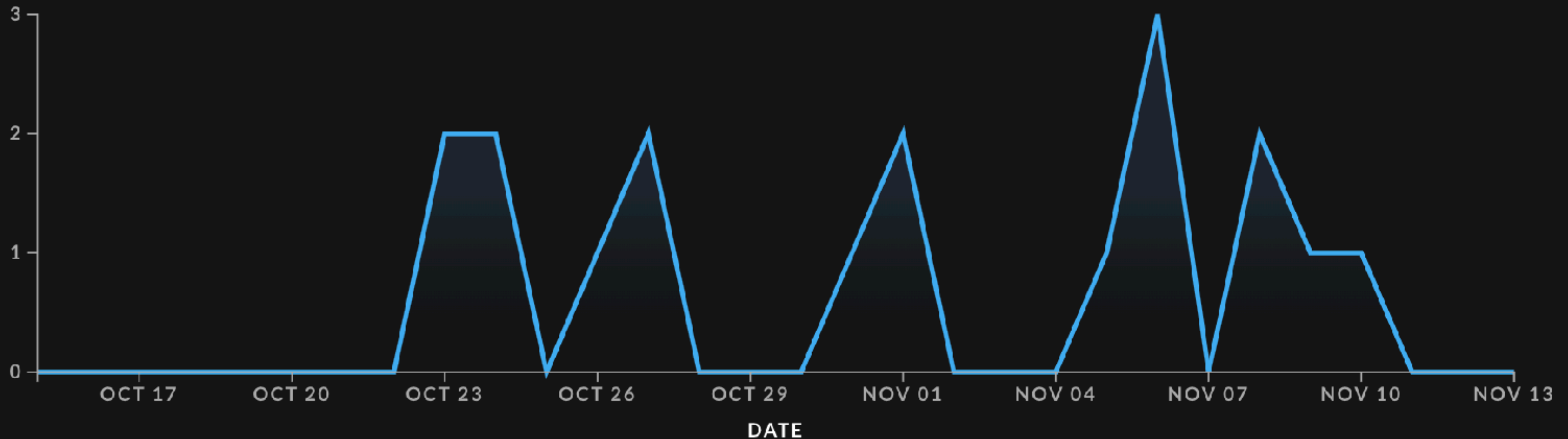
10 DAYS

30 DAYS

October 15, 2023 - November 13, 2023

13

UNIQUE IPS OBSERVED BY GREYNOISE



GREYNOISE TRENDS

JUNIPER JUNOS OS ARBITRARY FILE UPLOAD ATTEMPT

TAG INTENT

Malicious

TAG CATEGORY

Activity

CVES:

CVE-2023-36846

CVE-2023-36847

IP addresses with this tag have been observed attempting to exploit CVE-2023-36846 or CVE-2023-36847, an arbitrary file upload vulnerability in Juniper Junos OS SRX and EX Series.

3 DAYS

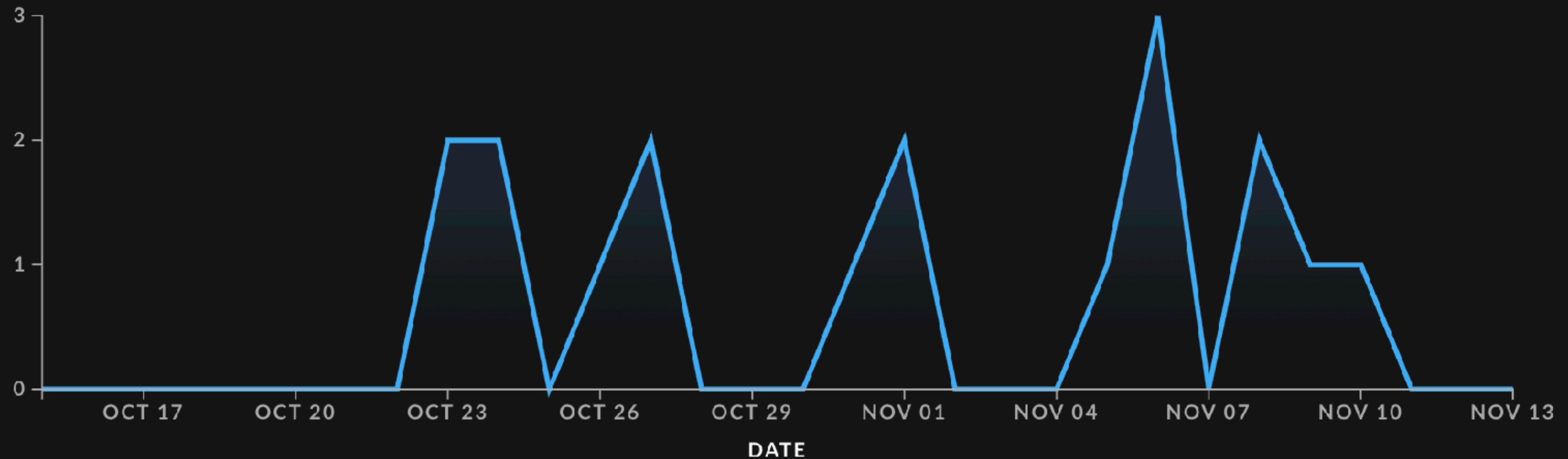
10 DAYS

• 30 DAYS

October 15, 2023 - November 13, 2023

13

UNIQUE IPS OBSERVED BY GREYNOISE



C H

<https://www.cyber.gov.au/smallbusiness/business-continuity-in-a-box>

[Home](#) > [Business Continuity in a Box](#)

Business Continuity in a Box

Content complexity

Advanced ● ● ●



First published: 10 Nov 2023

Last updated: 10 Nov 2023

Content written for



Small & medium business

Attachments



ACSC Business Continuity in a Box - Overview

433KB .pdf



ACSC Business Continuity in a

On this page

[Disclaimer](#)

[Overview](#)

[Why use Business Continuity in a Box?](#)

[Is Business Continuity in a Box right for your organisation?](#)

[How does Business Continuity in a Box fit into a cyber incident response?](#)

[Continuity of Communications](#)

[Continuity of Applications](#)

[Contact](#)

[Back to top](#)

<https://www.cyber.gov.au/smallbusiness/business-continuity-in-a-box>

[Home](#) > [Business Continuity in a Box](#)

Comprised of two core components—Continuity of Communications and Continuity of Applications—Business Continuity in a Box is designed for situations where the availability or integrity of an organization’s data and/or systems has been compromised. The core components focus on keeping communications flowing during an incident and establishing interim business-critical applications.

Attachments

 **ACSC Business Continuity in a Box - Overview**
433KB .pdf

 ACSC Business Continuity in a

[Is Business Continuity in a Box right for your organisation?](#)

[How does Business Continuity in a Box fit into a cyber incident response?](#)

[Continuity of Communications](#)

[Continuity of Applications](#)

[Contact](#)

[Back to top](#)



Securing the Software Supply Chain: Recommended Practices for Software Bill of Materials Consumption



Enduring Security Framework
November 2023



The guide provides best practices for developers, suppliers, and customers to ensure a secure software supply chain, including managing open source software and software bills of materials (SBOMs). The use of SBOMs is emphasized as they provide transparency, improve software asset management, and help address vulnerabilities. The document also discusses risk scoring and the factors that contribute to it, such as vulnerabilities, licenses, community support, and dependencies.

Key findings include the prevalence of open source vulnerabilities and the importance of patch management and vulnerability management.



Storm ⚡ Watch