Dateline: 2023-10-31

GREYNOISE LABS

STORM WATCH

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

Storm ⚡ Watch by GreyNoise Intelligence

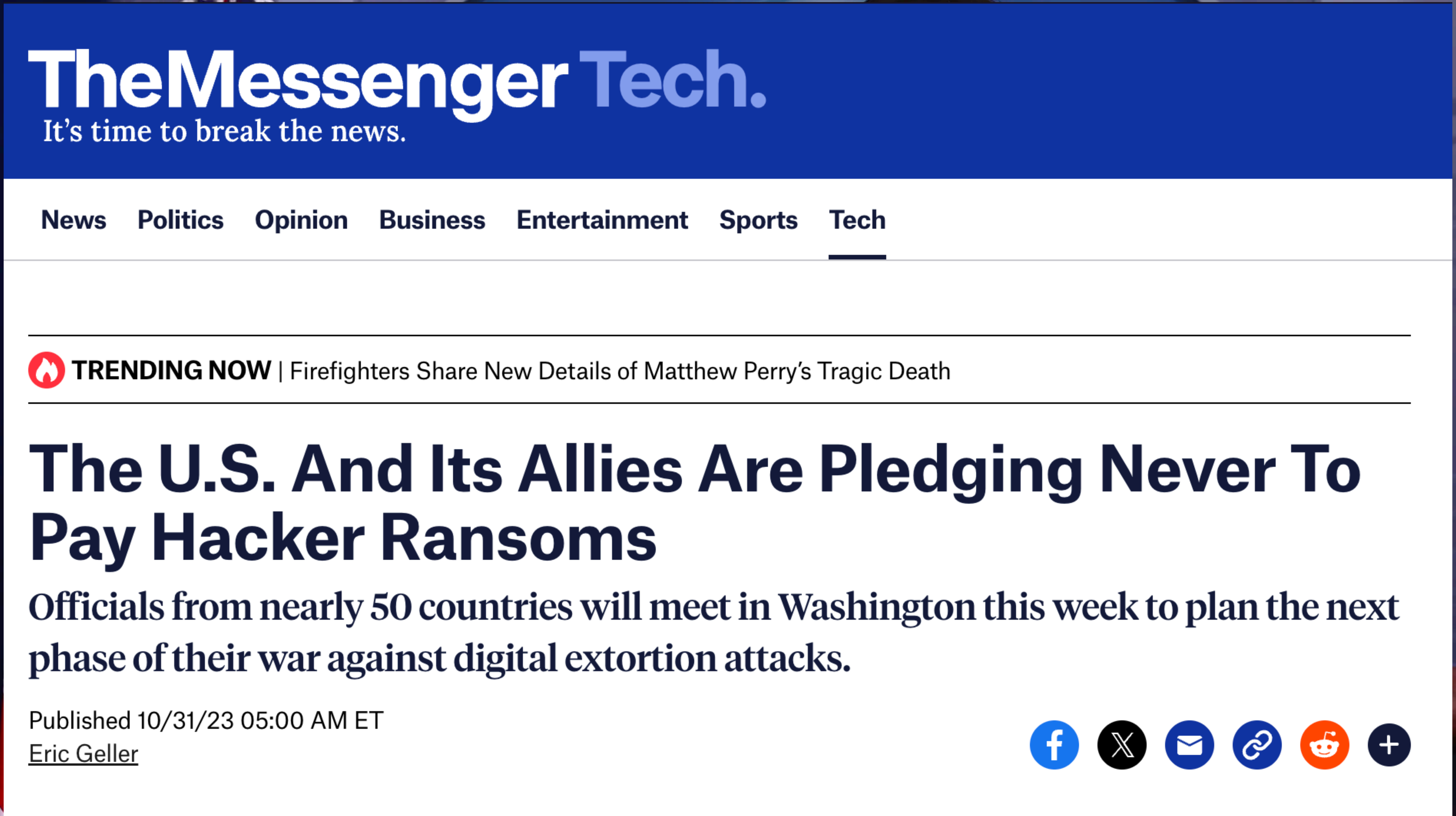
GreyNoise Intelligence

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://themessenger.com/tech/ransomware-us-international-hacking-ransom-pledge



TheMessenger Tech.

It’s time to break the news.

TRENDING NOW | Firefighters Share New Details of Matthew Perry’s Tragic Death

The U.S. And Its Allies Are Pledging Never To Pay Hacker Ransoms

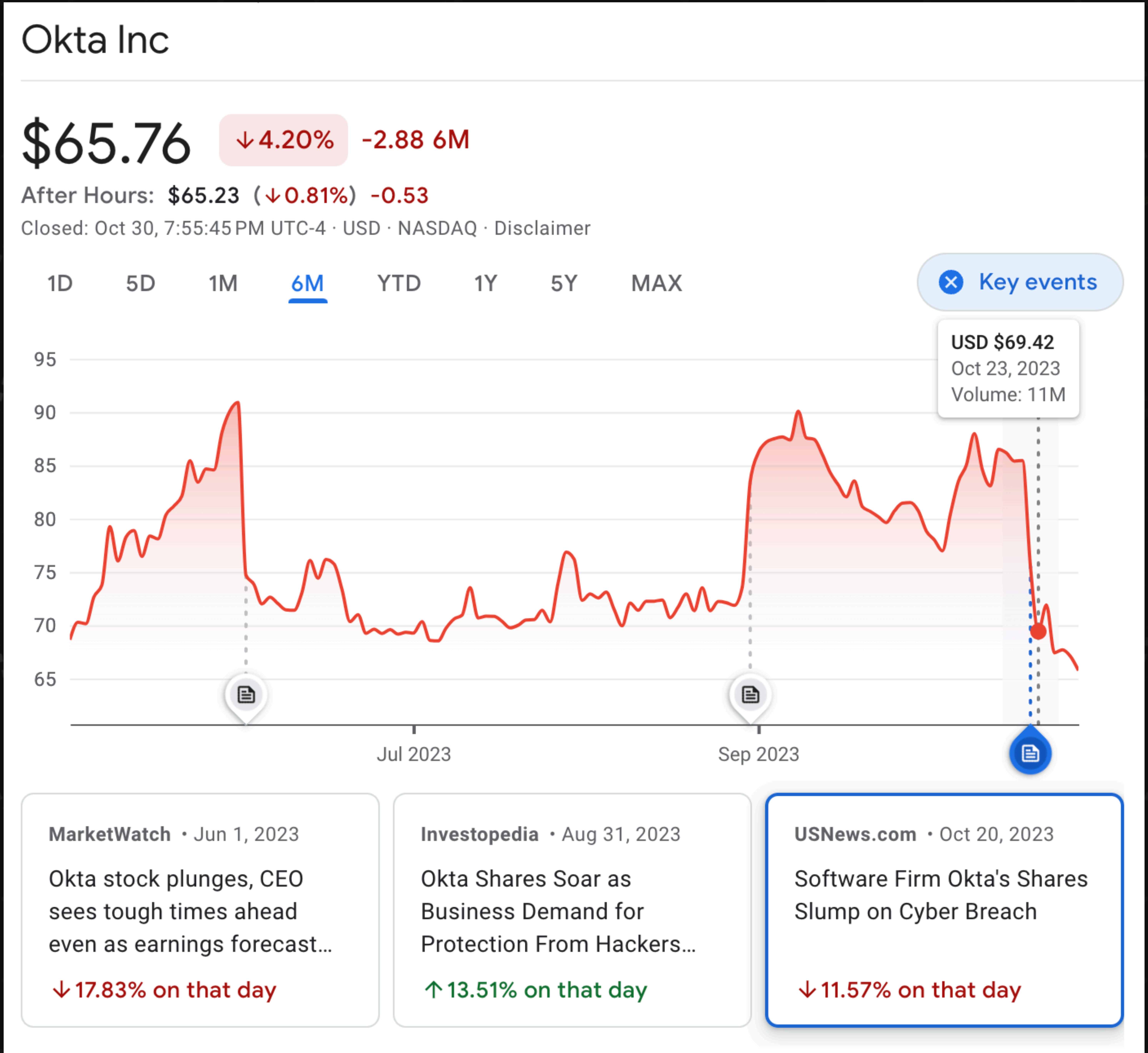
Officials from nearly 50 countries will meet in Washington this week to plan the next phase of their war against digital extortion attacks.

Published 10/31/23 05:00 AM ET

Eric Geller

BACK TO THE FUTURE
OUTATIME

https://www.bleepingcomputer.com/news/security/1password-discloses-security-incident-linked-to-okta-breach/



Okta Inc

$65.76 ↓4.20% -2.88 6M

After Hours: $65.23 (↓0.81%) -0.53

Closed: Oct 30, 7:55:45 PM UTC-4 · USD · NASDAQ · Disclaimer

MarketWatch • Jun 1, 2023

Okta stock plunges, CEO sees tough times ahead even as earnings forecast...

↓17.83% on that day

Investopedia • Aug 31, 2023

Okta Shares Soar as Business Demand for Protection From Hackers...

↑13.51% on that day

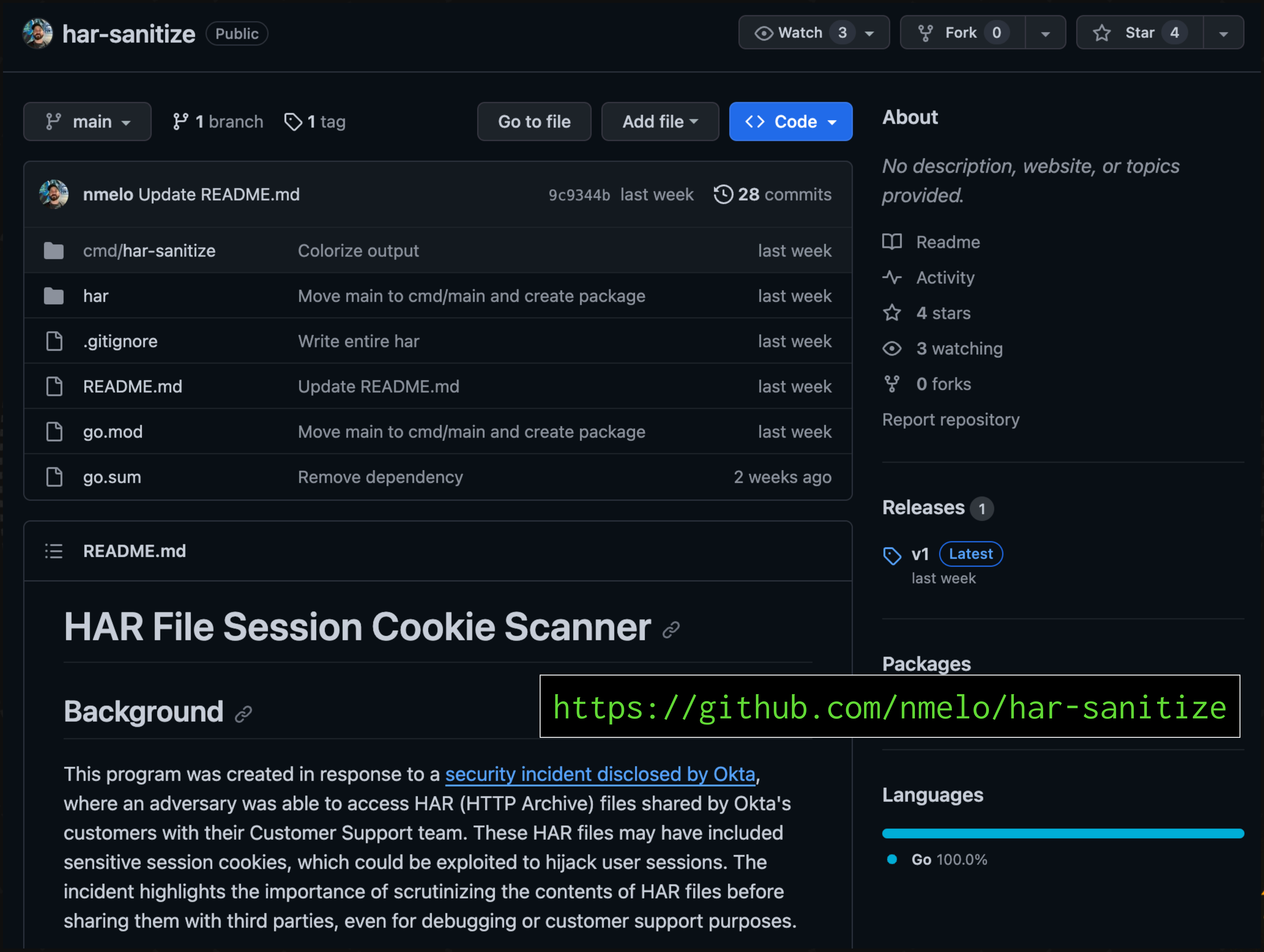
USNews.com • Oct 20, 2023

Software Firm Okta's Shares Slump on Cyber Breach

↓11.57% on that day

GREYNOISE LABS

STORM WATCH



nmelo Update README.md 9c9344b last week 28 commits

cmd/har-sanitize	Colorize output	last week
har	Move main to cmd/main and create package	last week
.gitignore	Write entire har	last week
README.md	Update README.md	last week
go.mod	Move main to cmd/main and create package	last week
go.sum	Remove dependency	2 weeks ago

README.md

HAR File Session Cookie Scanner

Background

This program was created in response to a security incident disclosed by Okta, where an adversary was able to access HAR (HTTP Archive) files shared by Okta's customers with their Customer Support team. These HAR files may have included sensitive session cookies, which could be exploited to hijack user sessions. The incident highlights the importance of scrutinizing the contents of HAR files before sharing them with third parties, even for debugging or customer support purposes.

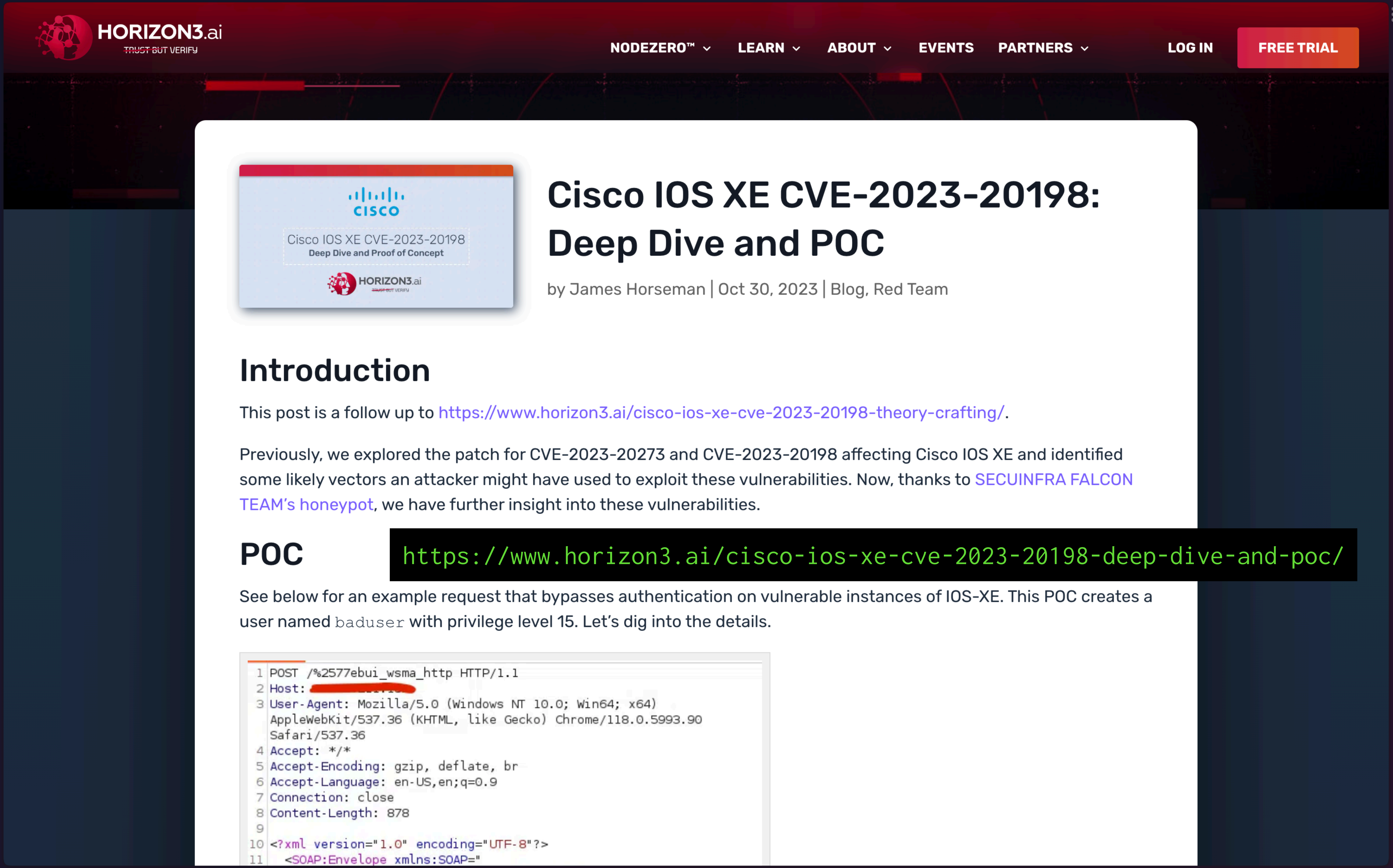
About

No description, website, or topics provided.

https://github.com/nmelo/har-sanitize

GREYNOIS LABS

WATCH



Cisco IOS XE CVE-2023-20198: Deep Dive and POC

by James Horseman | Oct 30, 2023 | Blog, Red Team

Introduction

This post is a follow up to https://www.horizon3.ai/cisco-ios-xe-cve-2023-20198-theory-crafting/.

Previously, we explored the patch for CVE-2023-20273 and CVE-2023-20198 affecting Cisco IOS XE and identified some likely vectors an attacker might have used to exploit these vulnerabilities. Now, thanks to SECUINFRA FALCON TEAM's honeypot, we have further insight into these vulnerabilities.

POC

https://www.horizon3.ai/cisco-ios-xe-cve-2023-20198-deep-dive-and-poc/

See below for an example request that bypasses authentication on vulnerable instances of IOS-XE. This POC creates a user named baduser with privilege level 15. Let's dig into the details.

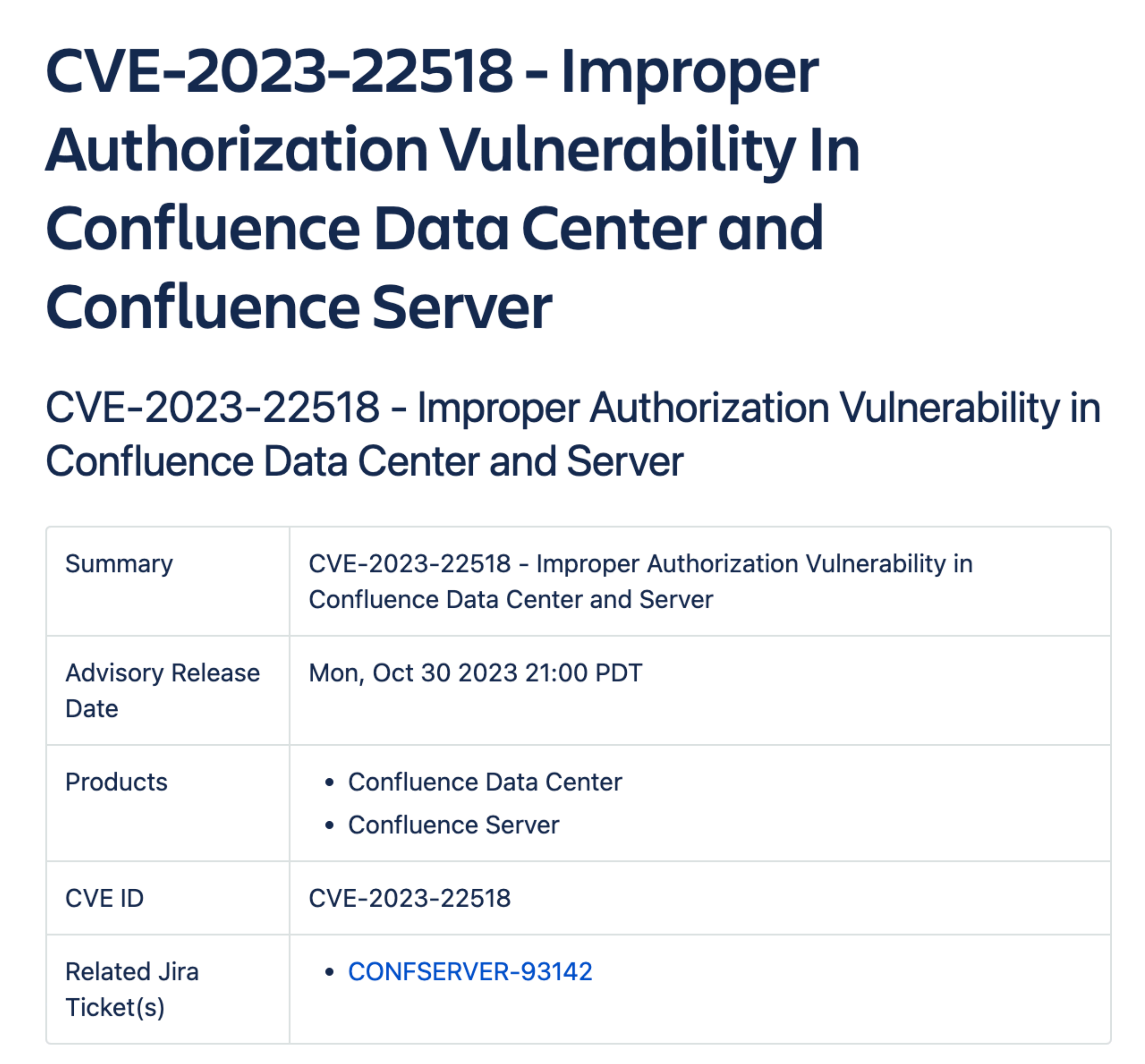
```
POST /%2577ebui_wsma_http HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.90
Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Length: 878

<?xml version="1.0" encoding="UTF-8"?>
  <SOAP:Envelope xmlns:SOAP="
```

AND NOW
BACK TO OUR
REGULARLY
SCHEDULED
PROGRAMMING

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

An Important Message from Bala Sathiamurthy, Chief Information Security Officer (CISO)

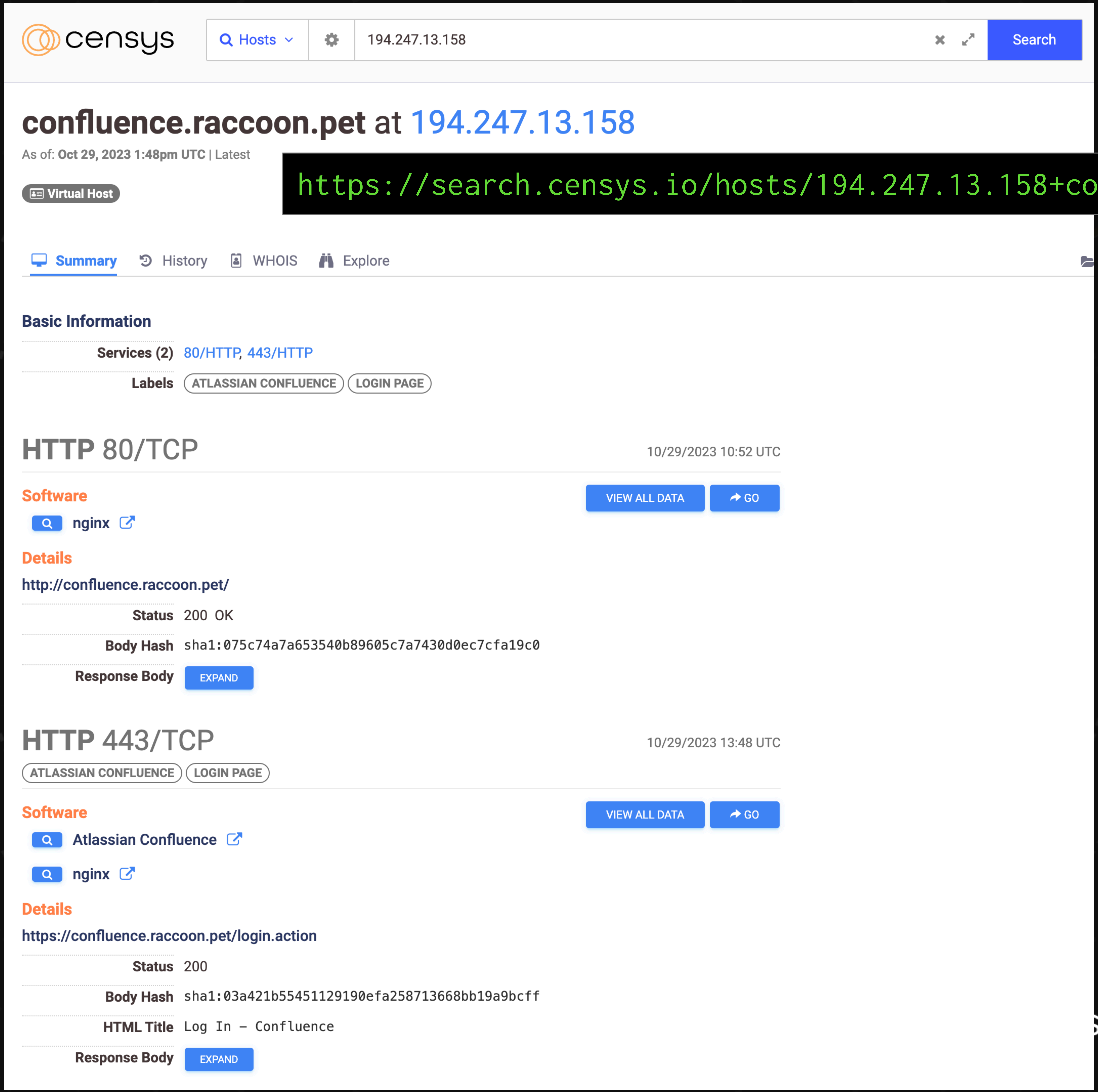
As part of our continuous security assessment processes, we have discovered that **Confluence Data Center and Server customers are vulnerable to significant data loss if exploited by an unauthenticated attacker.** There are no reports of active exploitation at this time; however, customers must take immediate action to protect their instances. Please read the Critical Security Advisory below for instructions and vulnerability details.a



CVE-2023-22518 - Improper Authorization Vulnerability In Confluence Data Center and Confluence Server

CVE-2023-22518 - Improper Authorization Vulnerability in Confluence Data Center and Server

Summary	CVE-2023-22518 - Improper Authorization Vulnerability in Confluence Data Center and Server
Advisory Release Date	Mon, Oct 30 2023 21:00 PDT
Products	• Confluence Data Center • Confluence Server
CVE ID	CVE-2023-22518
Related Jira Ticket(s)	• CONFSERVER-93142



https://search.censys.io/hosts/194.247.13.158+confluence.raccoon.pet

confluence.raccoon.pet at 194.247.13.158

As of: Oct 29, 2023 1:48pm UTC | Latest

Basic Information

Services (2)	80/HTTP, 443/HTTP
Labels	ATLASSIAN CONFLUENCE LOGIN PAGE

HTTP 80/TCP

10/29/2023 10:52 UTC

Software

nginx

Details

http://confluence.raccoon.pet/

Status	200 OK
Body Hash	sha1:075c74a7a653540b89605c7a7430d0ec7cfa19c0
Response Body	EXPAND

HTTP 443/TCP

10/29/2023 13:48 UTC

ATLASSIAN CONFLUENCE LOGIN PAGE

Software

Atlassian Confluence

nginx

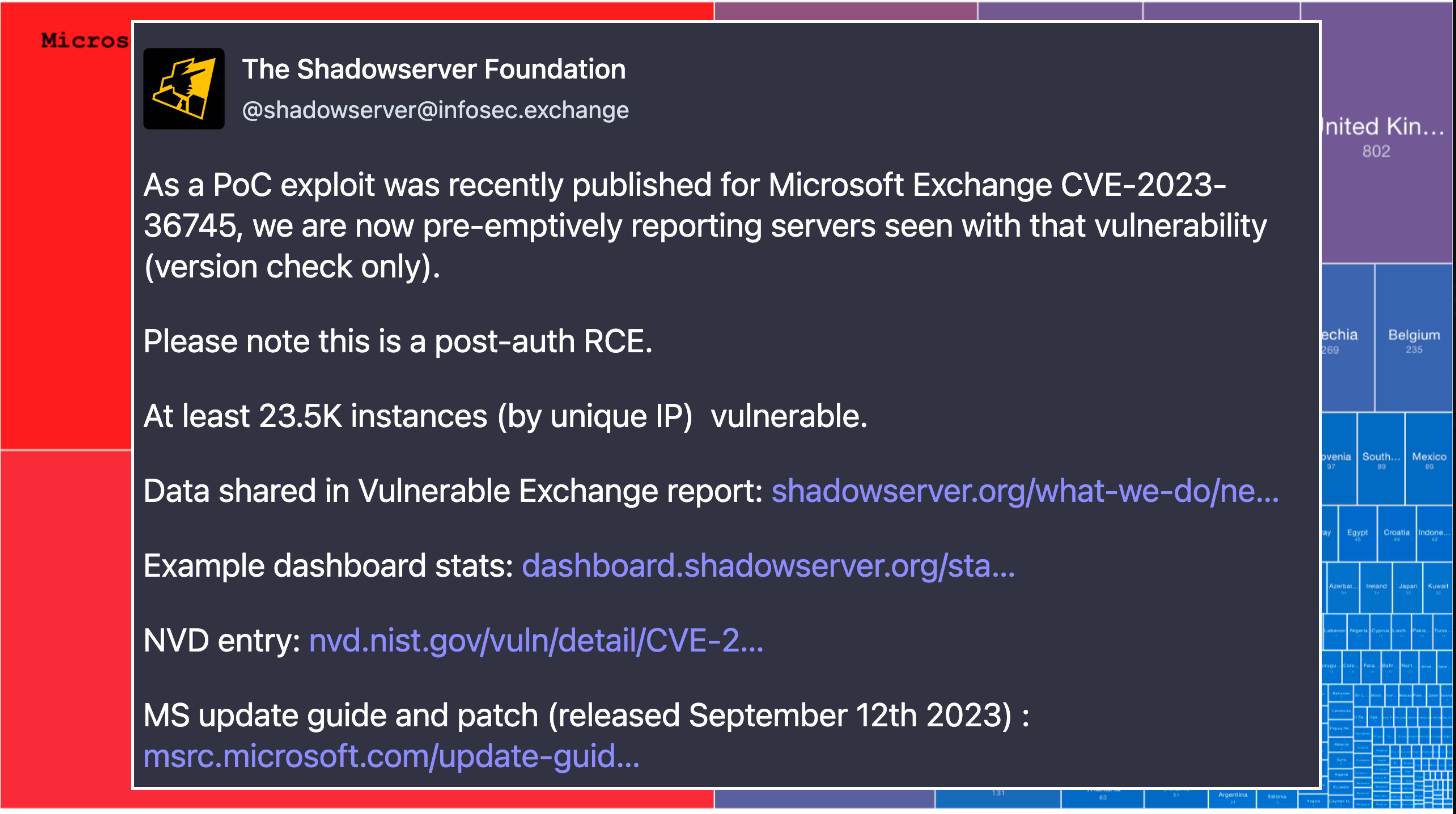
Details

https://confluence.raccoon.pet/login.action

Status	200
Body Hash	sha1:03a421b55451129190efa258713668bb19a9bcff
HTML Title	Log In - Confluence
Response Body	EXPAND

SHADOWSERVER

`https://infosec.exchange/@shadowserver/111320622091219330`



The Shadowserver Foundation
@shadowserver@infosec.exchange

As a PoC exploit was recently published for Microsoft Exchange CVE-2023-36745, we are now pre-emptively reporting servers seen with that vulnerability (version check only).

Please note this is a post-auth RCE.

At least 23.5K instances (by unique IP) vulnerable.

Data shared in Vulnerable Exchange report: shadowserver.org/what-we-do/ne…

Example dashboard stats: dashboard.shadowserver.org/sta…

NVD entry: nvd.nist.gov/vuln/detail/CVE-2…

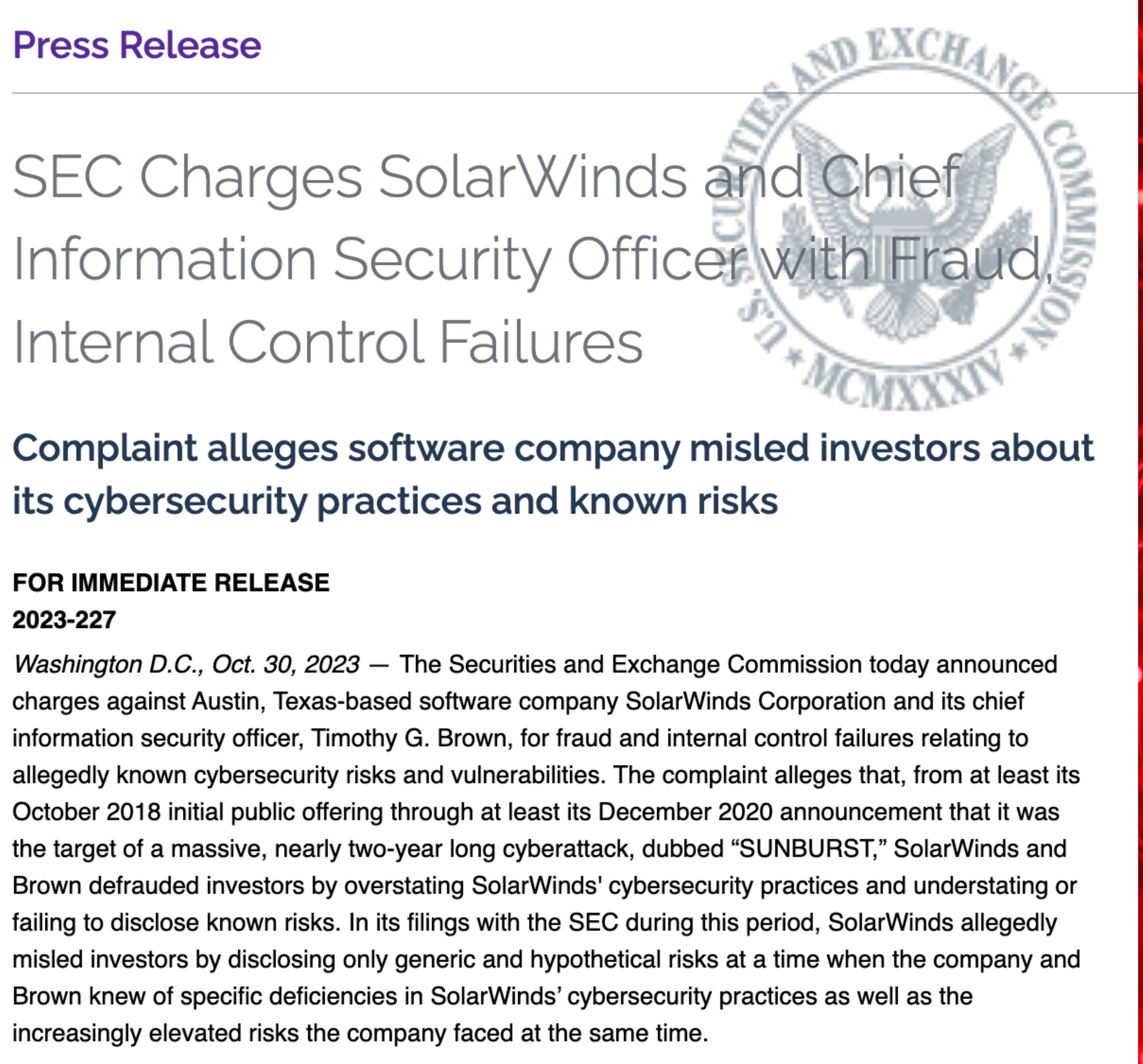
MS update guide and patch (released September 12th 2023) : msrc.microsoft.com/update-guid…

https://www.bleepingcomputer.com/news/security/critical-rce-flaws-found-in-solarwinds-access-audit-solution/

Remote unauthenticated attackers can execute arbitrary code in the context of SYSTEM Due To…

- CVE-2023-35182 (9.8): the deserialization of untrusted data in the ‘createGlobalServerChannelInternal’ method
- CVE-2023-35185 (9.8): a lack of validation of user-supplied paths in the ‘OpenFile’ method
- CVE-2023-35187 (9.8): without authentication due to lack of validation of user-supplied paths in the ‘OpenClientUpdateFile’ method

https://www.sec.gov/news/press-release/2023-227



Press Release

SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures

Complaint alleges software company misled investors about its cybersecurity practices and known risks

FOR IMMEDIATE RELEASE
2023-227

Washington D.C., Oct. 30, 2023 — The Securities and Exchange Commission today announced charges against Austin, Texas-based software company SolarWinds Corporation and its chief information security officer, Timothy G. Brown, for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities. The complaint alleges that, from at least its October 2018 initial public offering through at least its December 2020 announcement that it was the target of a massive, nearly two-year long cyberattack, dubbed "SUNBURST," SolarWinds and Brown defrauded investors by overstating SolarWinds' cybersecurity practices and understating or failing to disclose known risks. In its filings with the SEC during this period, SolarWinds allegedly misled investors by disclosing only generic and hypothetical risks at a time when the company and Brown knew of specific deficiencies in SolarWinds' cybersecurity practices as well as the increasingly elevated risks the company faced at the same time.

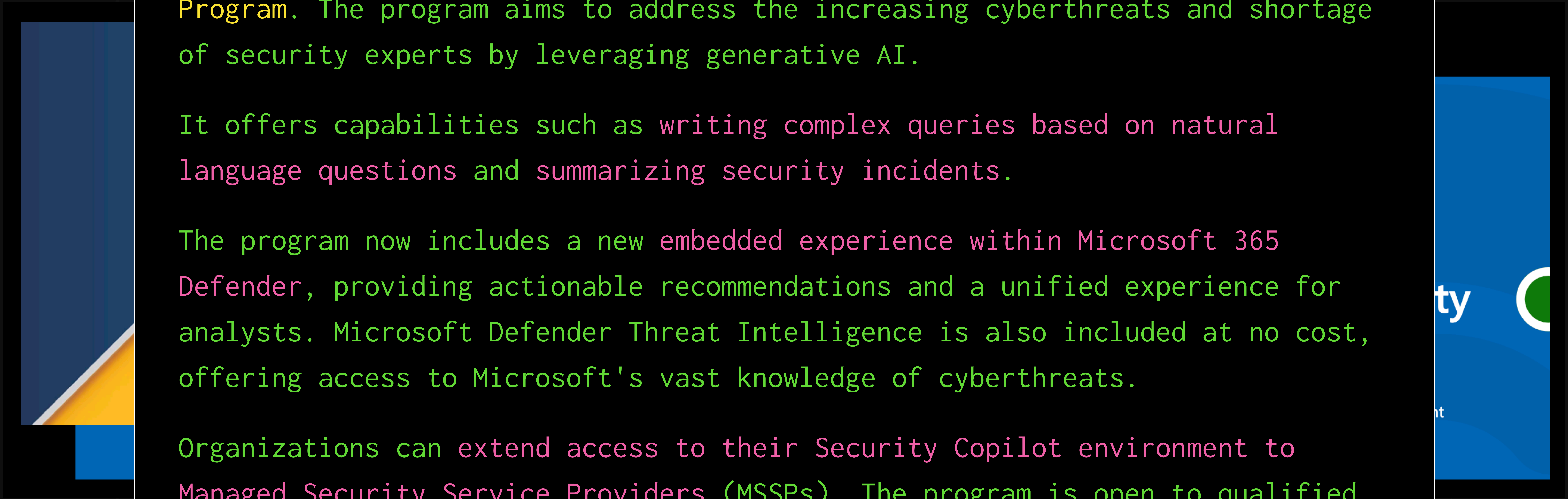
https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/

Octo Tempest is a financially motivated threat actor group that poses a significant danger to organizations across various industries such as natural resources, gaming, hospitality, and financial services. They employ a wide range of tactics, including adversary-in-the-middle techniques, social engineering, and SIM swapping.

Initially, they sold SIM swaps and performed account takeovers to steal cryptocurrency. Later, they began extorting victim organizations for stolen data and even resorted to physical threats. In 2023, they became an affiliate of ALPHV/BlackCat, a ransomware operation, and started deploying ransomware payloads.

They establish persistence within organizations using publicly available tools and exfiltrate data using anonymous file-hosting services. The document also provides guidelines for organizations to defend against Octo Tempest's activities, including aligning privileges, implementing conditional access policies, and educating users.

https://www.microsoft.com/en-us/security/blog/2023/10/19/microsoft-security-copilot-early-access-program-harnessing-generative-ai-to-empower-security-teams/



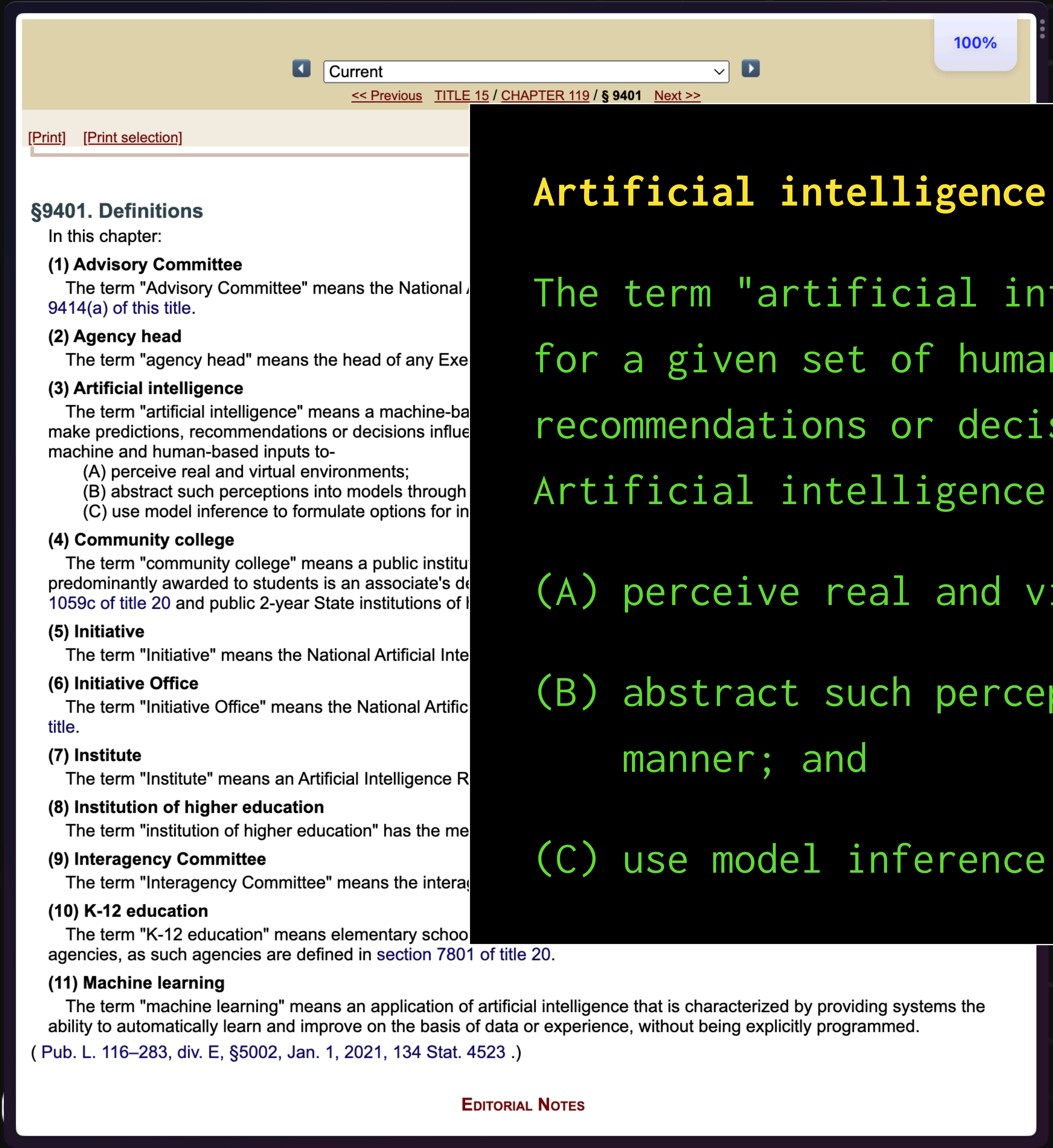
Microsoft has announced the availability of its Security Copilot Early Access Program. The program aims to address the increasing cyberthreats and shortage of security experts by leveraging generative AI.

It offers capabilities such as writing complex queries based on natural language questions and summarizing security incidents.

The program now includes a new embedded experience within Microsoft 365 Defender, providing actionable recommendations and a unified experience for analysts. Microsoft Defender Threat Intelligence is also included at no cost, offering access to Microsoft's vast knowledge of cyberthreats.

Organizations can extend access to their Security Copilot environment to Managed Security Service Providers (MSSPs). The program is open to qualified customers, and interested parties can sign up for early access.

http://uscode.house.gov/view.xhtml?req=(title:15 section:9401 edition:prelim)


100%
Current
<< Previous TITLE 15 / CHAPTER 119 / § 9401 Next >>
[Print] [Print selection]

§9401. Definitions

In this chapter:

(1) Advisory Committee

The term "Advisory Committee" means the National
9414(a) of this title.

(2) Agency head

The term "agency head" means the head of any Exe

(3) Artificial intelligence

The term "artificial intelligence" means a machine-ba
make predictions, recommendations or decisions influe
machine and human-based inputs to-

(A) perceive real and virtual environments;
(B) abstract such perceptions into models through
(C) use model inference to formulate options for in

(4) Community college

The term "community college" means a public institu
predominantly awarded to students is an associate's de
1059c of title 20 and public 2-year State institutions of I

(5) Initiative

The term "Initiative" means the National Artificial Inte

(6) Initiative Office

The term "Initiative Office" means the National Artific
title.

(7) Institute

The term "Institute" means an Artificial Intelligence R

(8) Institution of higher education

The term "institution of higher education" has the me

(9) Interagency Committee

The term "Interagency Committee" means the intera

(10) K-12 education

The term "K-12 education" means elementary schoo
agencies, as such agencies are defined in section 7801 of title 20.

(11) Machine learning

The term "machine learning" means an application of artificial intelligence that is characterized by providing systems the ability to automatically learn and improve on the basis of data or experience, without being explicitly programmed.

(Pub. L. 116–283, div. E, §5002, Jan. 1, 2021, 134 Stat. 4523 .)

EDITORIAL NOTES

Artificial intelligence

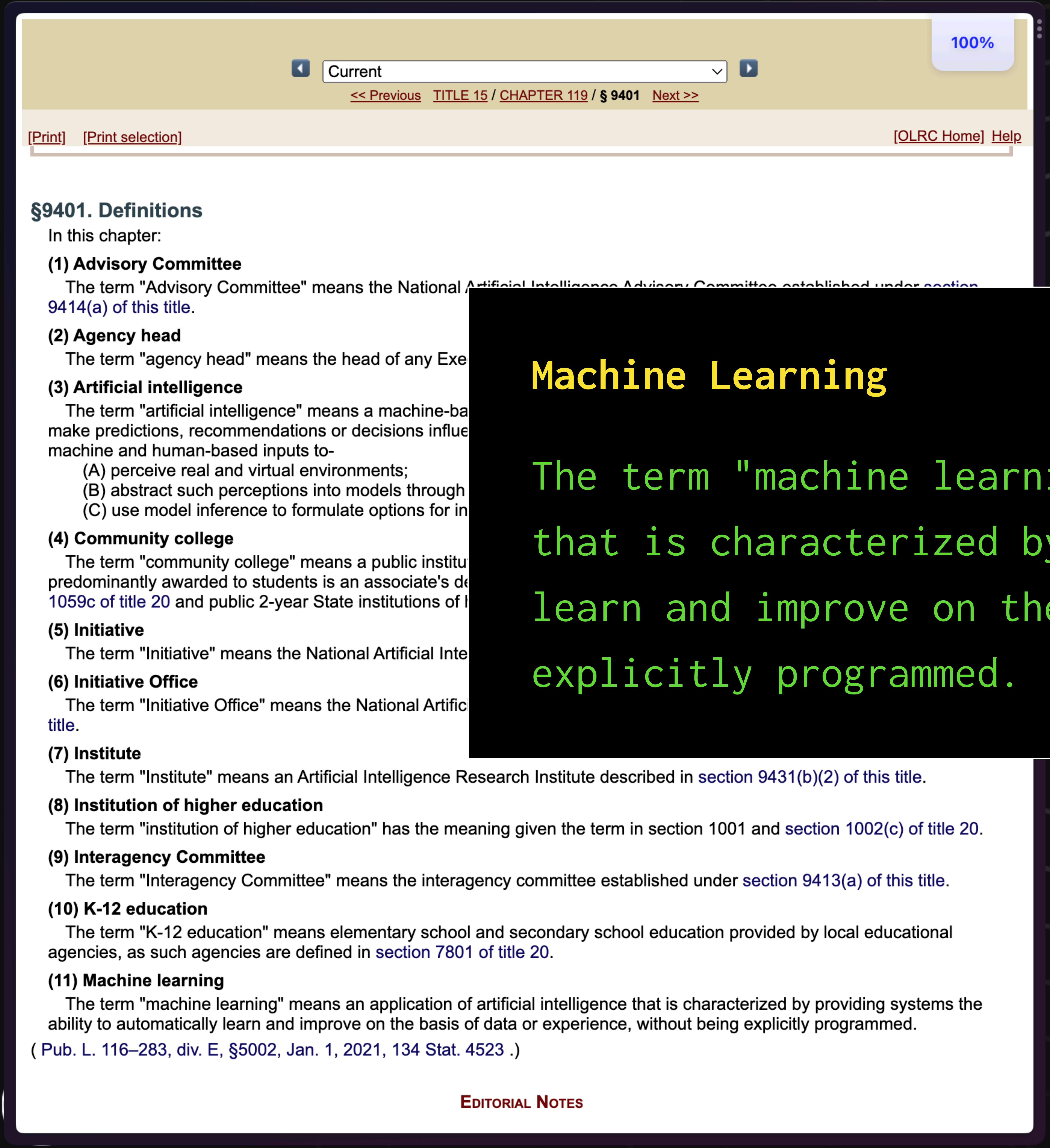
The term "artificial intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to-

(A) perceive real and virtual environments;

(B) abstract such perceptions into models through analysis in an automated manner; and

(C) use model inference to formulate options for information or action.

```
http://uscode.house.gov/view.xhtml?req=(title:15 section:9401 edition:prelim)
```



100%
Current
<< Previous TITLE 15 / CHAPTER 119 / § 9401 Next >>
[Print] [Print selection]
[OLRC Home] Help

§9401. Definitions

In this chapter:

(1) Advisory Committee

The term "Advisory Committee" means the National Artificial Intelligence Advisory Committee established under section 9414(a) of this title.

(2) Agency head

The term "agency head" means the head of any Exe

(3) Artificial intelligence

The term "artificial intelligence" means a machine-ba
make predictions, recommendations or decisions influe
machine and human-based inputs to-

(A) perceive real and virtual environments;
(B) abstract such perceptions into models through
(C) use model inference to formulate options for in

(4) Community college

The term "community college" means a public institu
predominantly awarded to students is an associate's de
1059c of title 20 and public 2-year State institutions of I

(5) Initiative

The term "Initiative" means the National Artificial Inte

(6) Initiative Office

The term "Initiative Office" means the National Artific
title.

(7) Institute

The term "Institute" means an Artificial Intelligence Research Institute described in section 9431(b)(2) of this title.

(8) Institution of higher education

The term "institution of higher education" has the meaning given the term in section 1001 and section 1002(c) of title 20.

(9) Interagency Committee

The term "Interagency Committee" means the interagency committee established under section 9413(a) of this title.

(10) K-12 education

The term "K-12 education" means elementary school and secondary school education provided by local educational agencies, as such agencies are defined in section 7801 of title 20.

(11) Machine learning

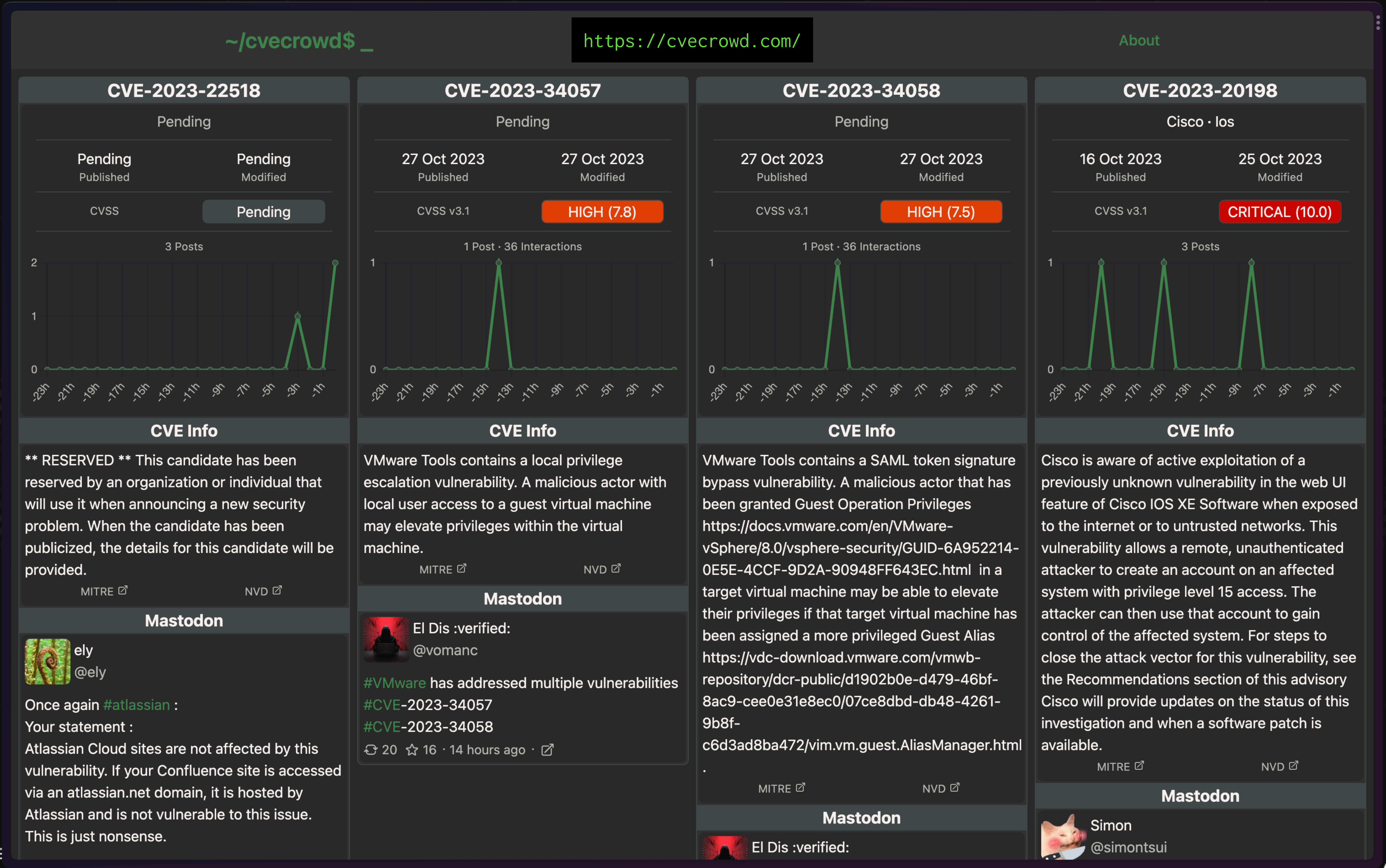
The term "machine learning" means an application of artificial intelligence that is characterized by providing systems the ability to automatically learn and improve on the basis of data or experience, without being explicitly programmed.

(Pub. L. 116–283, div. E, §5002, Jan. 1, 2021, 134 Stat. 4523 .)

EDITORIAL NOTES

Machine Learning

The term "machine learning" means an application of artificial intelligence that is characterized by providing systems the ability to automatically learn and improve on the basis of data or experience, without being explicitly programmed.



CVE-2023-22518

Pending

Pending	Pending
Published	Modified

CVSS Pending

3 Posts

CVE Info

** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

MITRE NVD

Mastodon

ely
@ely

Once again #atlassian :
Your statement :
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.
This is just nonsense.

CVE-2023-34057

Pending

27 Oct 2023	27 Oct 2023
Published	Modified

CVSS v3.1 HIGH (7.8)

1 Post · 36 Interactions

CVE Info

VMware Tools contains a local privilege escalation vulnerability. A malicious actor with local user access to a guest virtual machine may elevate privileges within the virtual machine.

MITRE NVD

Mastodon

El Dis :verified:
@vomanc

#VMware has addressed multiple vulnerabilities
#CVE-2023-34057
#CVE-2023-34058

20 ☆ 16 · 14 hours ago ·

CVE-2023-34058

Pending

27 Oct 2023	27 Oct 2023
Published	Modified

CVSS v3.1 HIGH (7.5)

1 Post · 36 Interactions

CVE Info

VMware Tools contains a SAML token signature bypass vulnerability. A malicious actor that has been granted Guest Operation Privileges https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-6A952214-0E5E-4CCF-9D2A-90948FF643EC.html in a target virtual machine may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias https://vdc-download.vmware.com/vmwb-repository/dcr-public/d1902b0e-d479-46bf-8ac9-cee0e31e8ec0/07ce8dbd-db48-4261-9b8f-c6d3ad8ba472/vim.vm.guest.AliasManager.html .

MITRE NVD

Mastodon

El Dis :verified:

CVE-2023-20198

Cisco · Ios

16 Oct 2023	25 Oct 2023
Published	Modified

CVSS v3.1 CRITICAL (10.0)

3 Posts

CVE Info

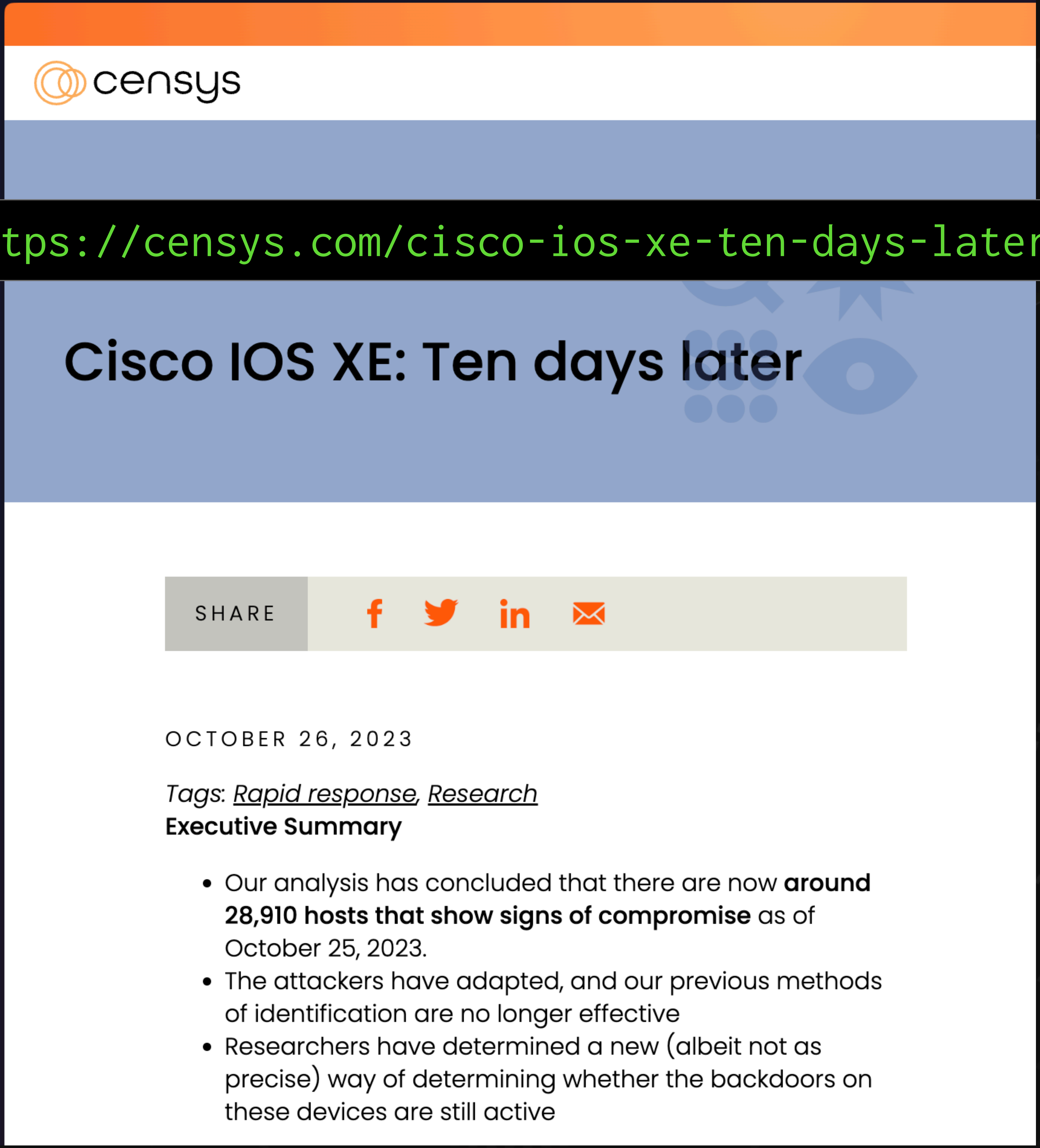
Cisco is aware of active exploitation of a previously unknown vulnerability in the web UI feature of Cisco IOS XE Software when exposed to the internet or to untrusted networks. This vulnerability allows a remote, unauthenticated attacker to create an account on an affected system with privilege level 15 access. The attacker can then use that account to gain control of the affected system. For steps to close the attack vector for this vulnerability, see the Recommendations section of this advisory Cisco will provide updates on the status of this investigation and when a software patch is available.

MITRE NVD

Mastodon

Simon
@simontsui

`https://censys.com/cisco-ios-xe-ten-days-later/`



censys

Cisco IOS XE: Ten days later

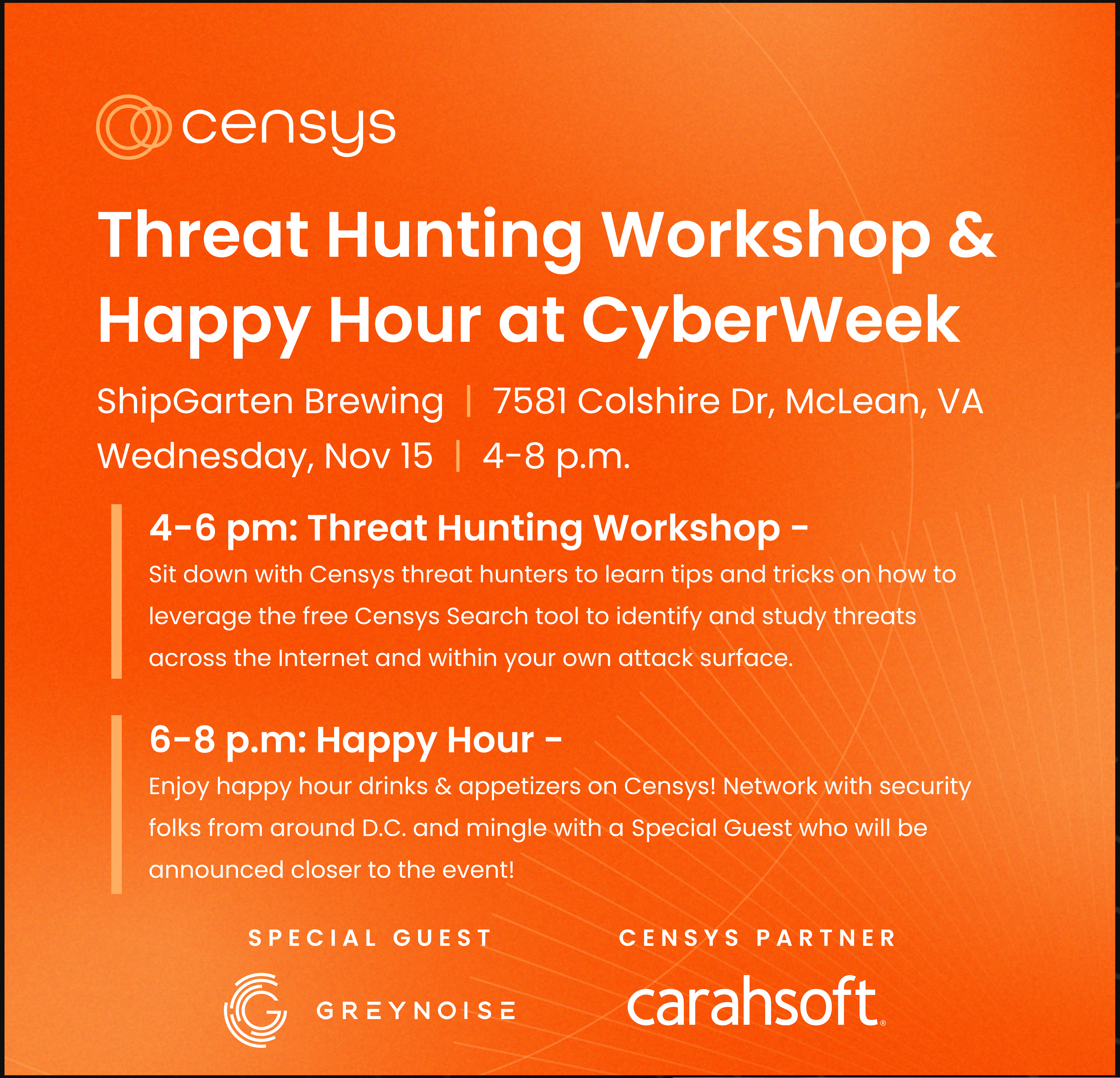
SHARE

OCTOBER 26, 2023

Tags: *Rapid response*, *Research*

Executive Summary

- Our analysis has concluded that there are now **around 28,910 hosts that show signs of compromise** as of October 25, 2023.
- The attackers have adapted, and our previous methods of identification are no longer effective
- Researchers have determined a new (albeit not as precise) way of determining whether the backdoors on these devices are still active



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 -

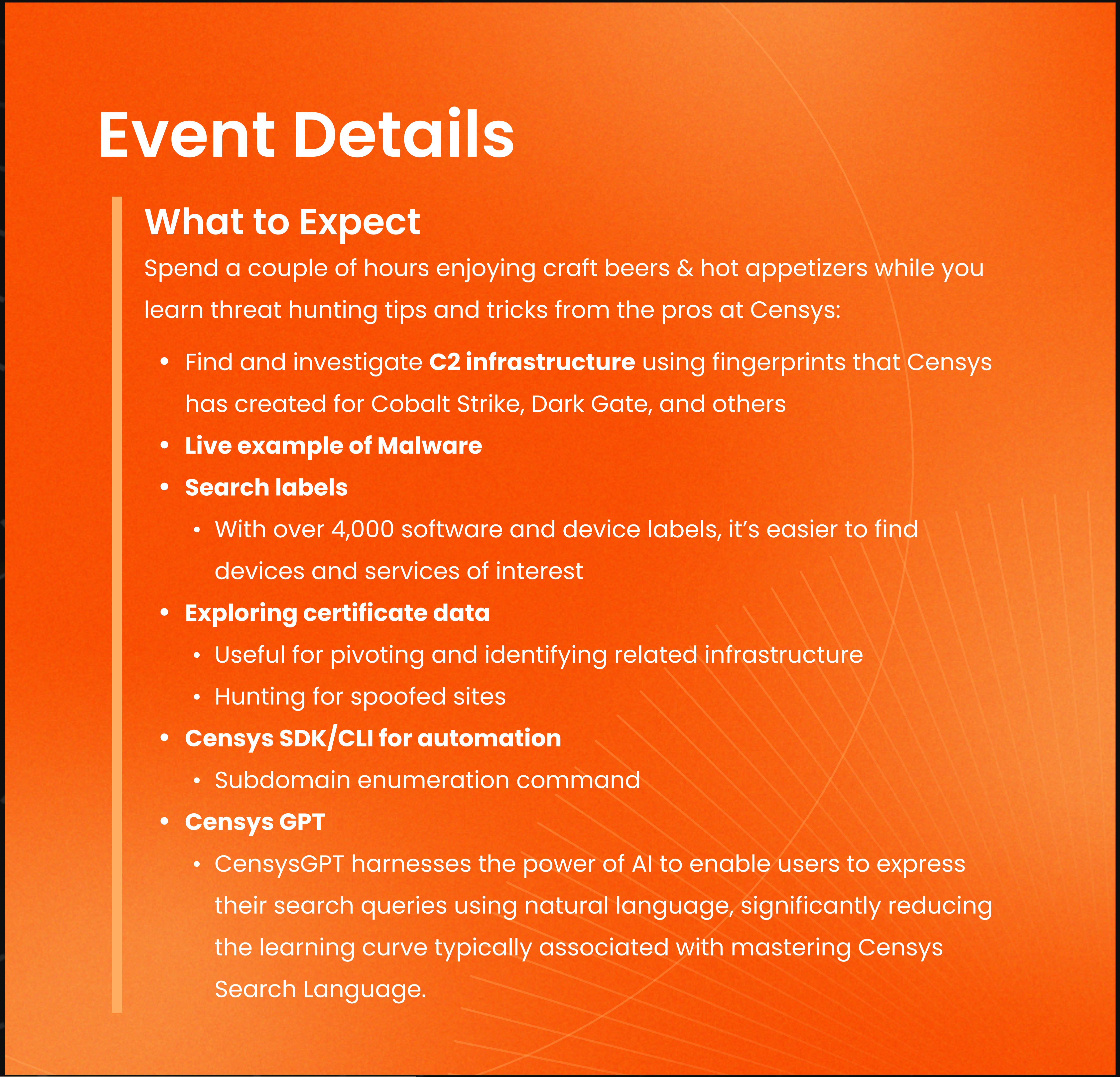
Enjoy happy hour drinks & appetizers on Censys! Network with security folks from around D.C. and mingle with a Special Guest who will be announced closer to the event!

SPECIAL GUEST

GREYNOISE

CENSYS PARTNER

carahsoft

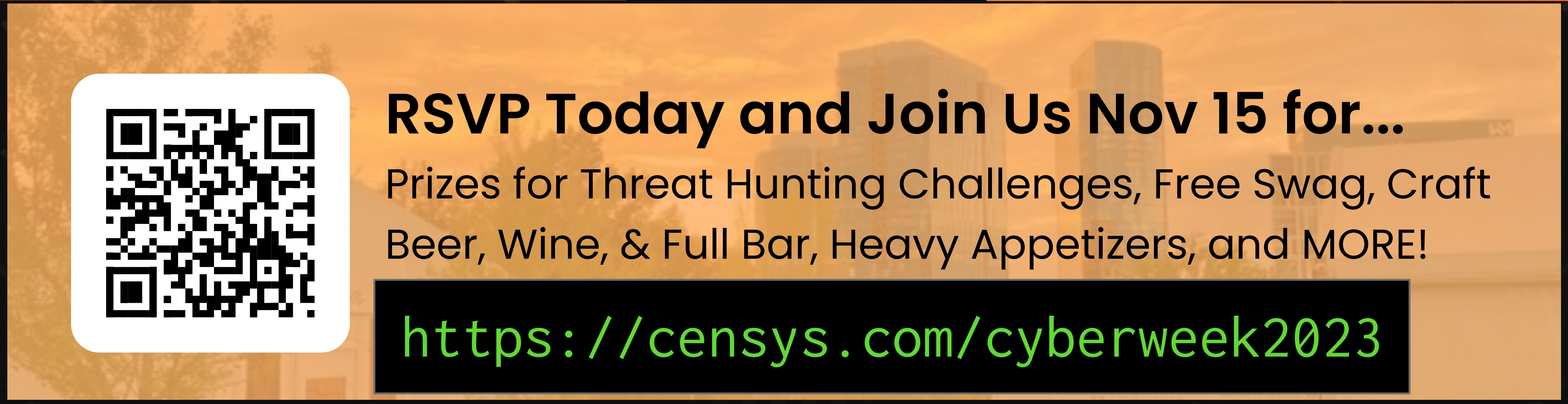


Event Details

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

VULNERABILITIES

CVE-2023-4966 Helps Usher In A Baker’s Dozen Of Citrix Tags To Further Help Organizations Mitigate Harm

Citrix's NetScaler ADC and NetScaler Gateway have, once more, been found to have multiple vulnerabilities, tracked as CVE-2023-4966 and CVE-2023-4967. Read this blog to get all the details.

ACTIVELY EXPLOITED

NEW VULN

Citrix ADC NetScaler

CVE-2023-4966

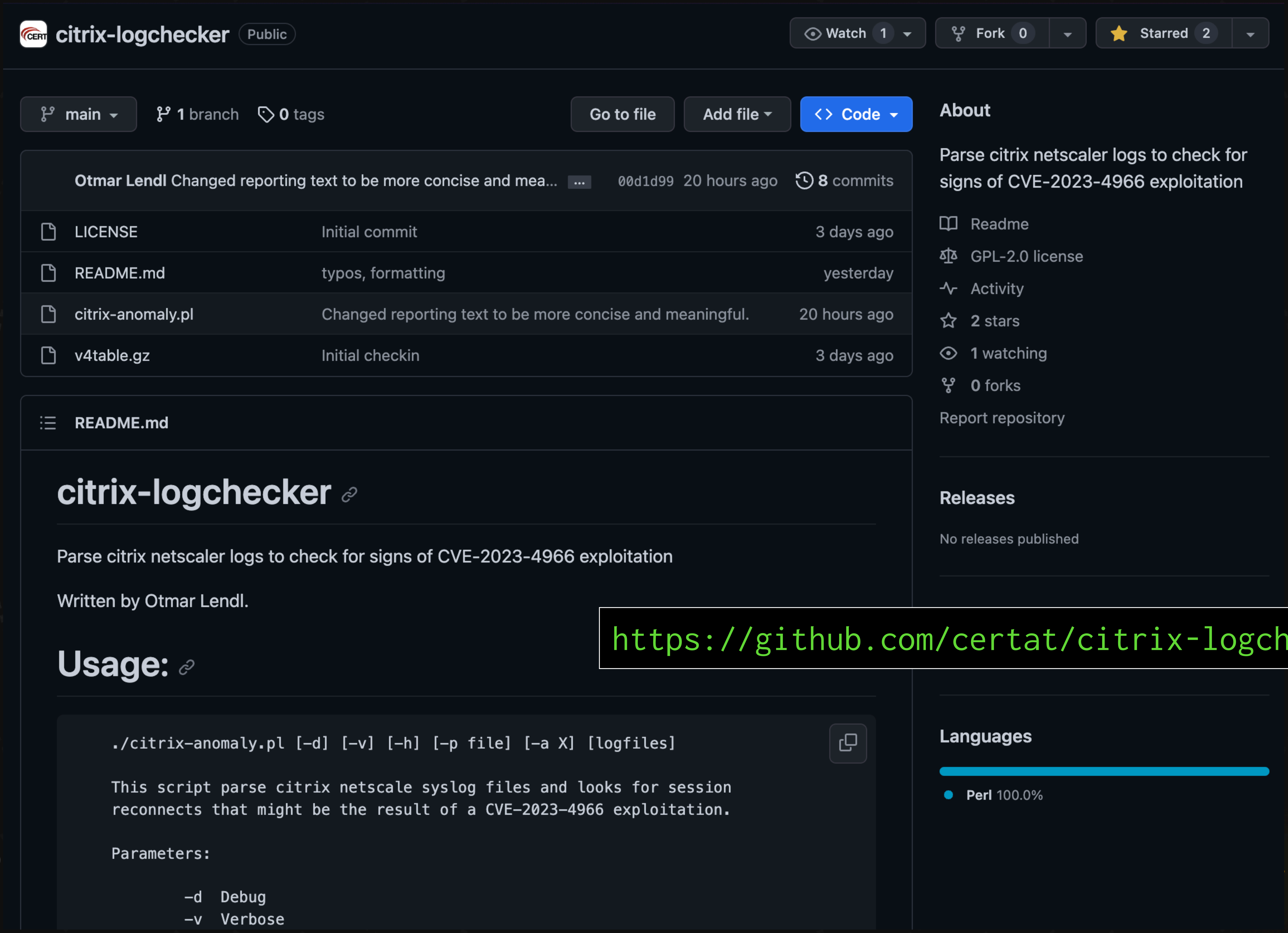
boB Rudis | Oct 26, 2023

https://www.greynoise.io/blog/cve-2023-4966-helps-usher-in-a-bakers-dozen-of-citrix-tags-to-further-help-organizations-mitigate-harm

https://viz.greynoise.io/tag/citrix-adc-netscaler-cve-2023-4966-information-disclosure-attempt?days=30

GREYNOISE LABS

STORM WATCH



Otmar Lendl Changed reporting text to be more concise and mea... 00d1d99 20 hours ago 8 commits

LICENSE	Initial commit	3 days ago
README.md	typos, formatting	yesterday
citrix-anomaly.pl	Changed reporting text to be more concise and meaningful.	20 hours ago
v4table.gz	Initial checkin	3 days ago

README.md

citrix-logchecker

Parse citrix netscaler logs to check for signs of CVE-2023-4966 exploitation

Written by Otmar Lendl.

Usage:

```
./citrix-anomaly.pl [-d] [-v] [-h] [-p file] [-a X] [logfiles]

This script parse citrix netscale syslog files and looks for session
reconnects that might be the result of a CVE-2023-4966 exploitation.

Parameters:

        -d  Debug
        -v  Verbose
```

About

Parse citrix netscaler logs to check for signs of CVE-2023-4966 exploitation

Readme
GPL-2.0 license
Activity
2 stars
1 watching
0 forks
Report repository

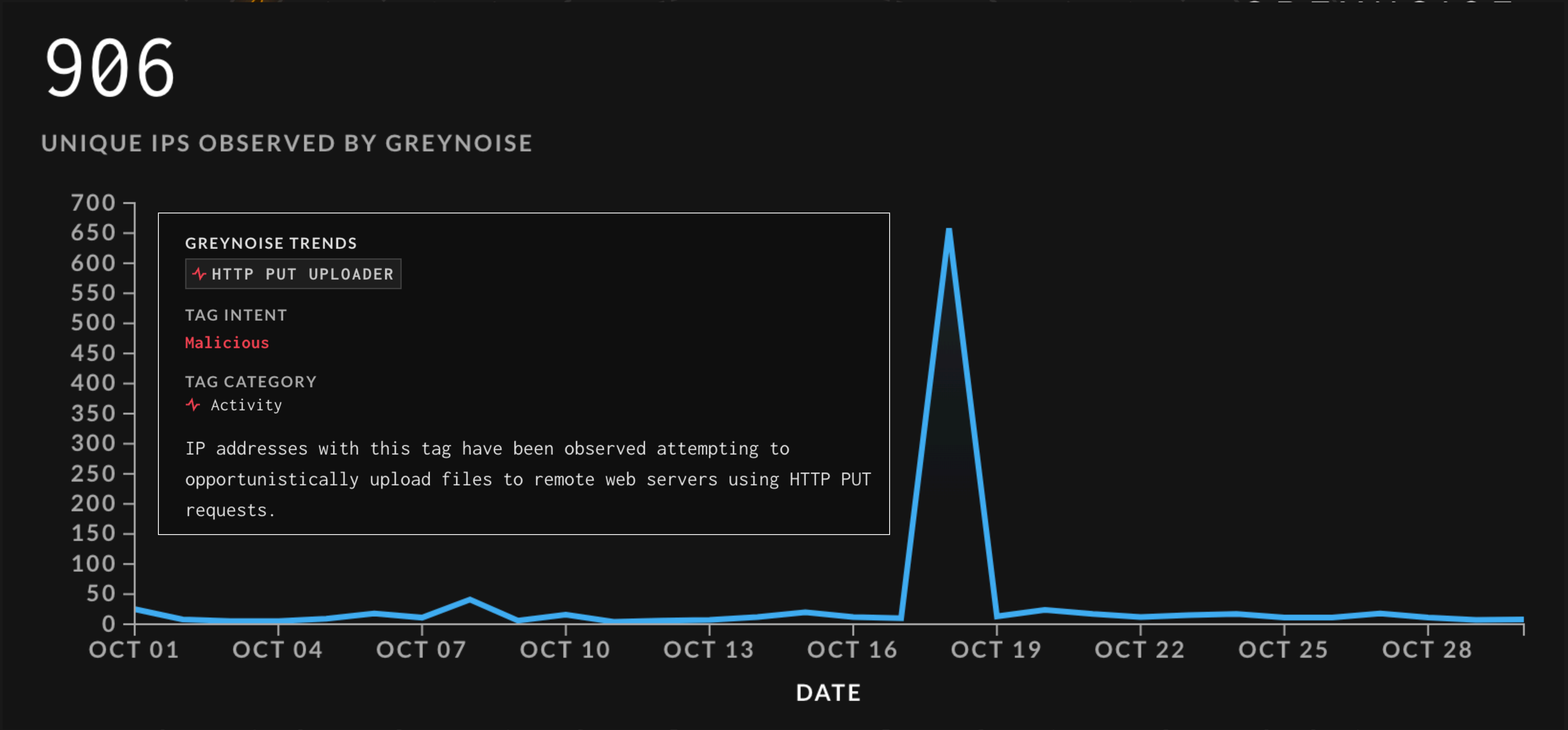
Releases

No releases published

Languages

Perl 100.0%

https://github.com/certat/citrix-logchecker



906

UNIQUE IPS OBSERVED BY GREYNOISE

GREYNOISE TRENDS

HTTP PUT UPLOADER

TAG INTENT

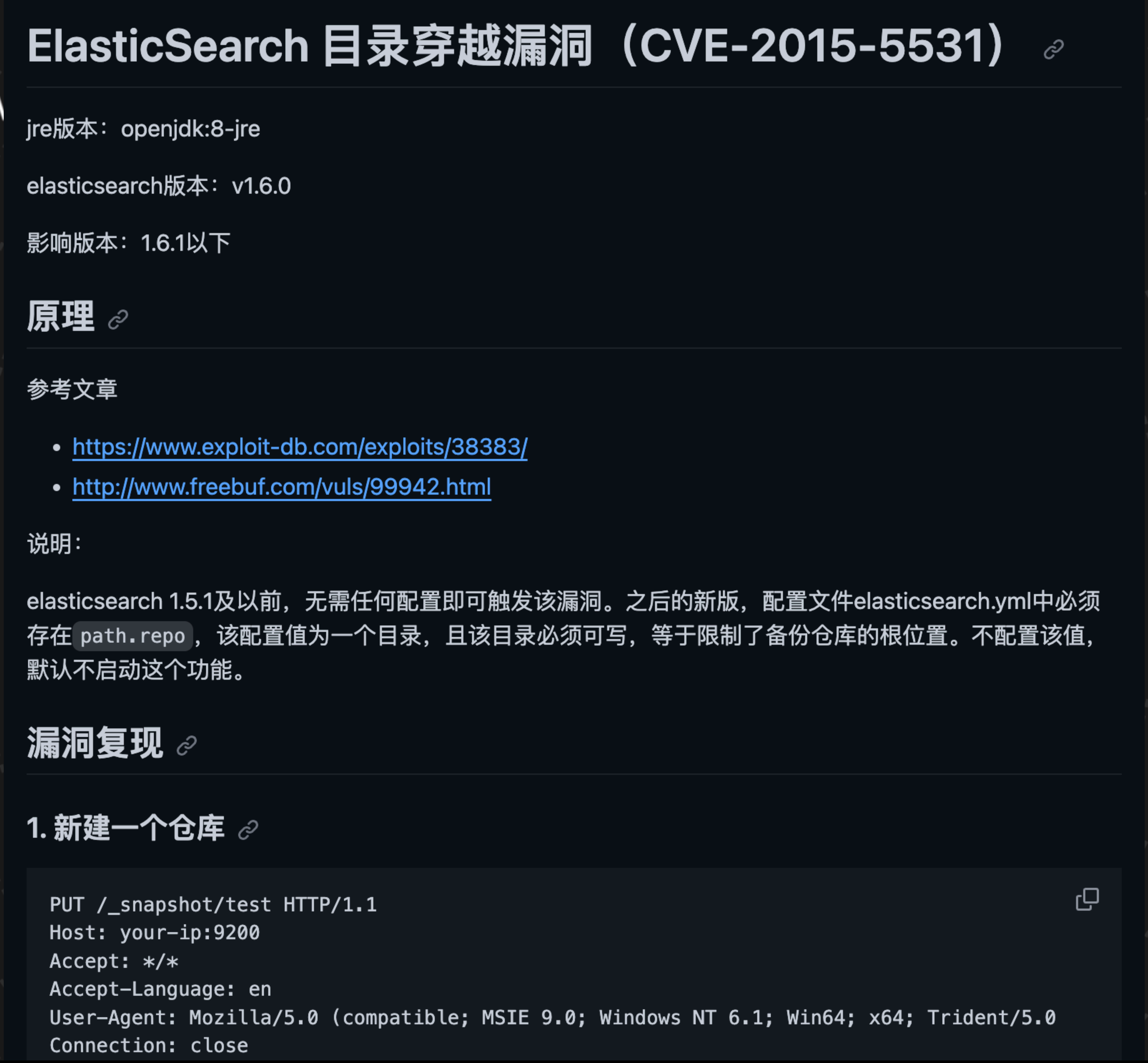
Malicious

TAG CATEGORY

Activity

IP addresses with this tag have been observed attempting to opportunistically upload files to remote web servers using HTTP PUT requests.

https://viz.greynoise.io/tag/http-put-uploader-scanner?days=10



ElasticSearch 目录穿越漏洞（CVE-2015-5531）

jre版本：openjdk:8-jre

elasticsearch版本：v1.6.0

影响版本：1.6.1以下

原理

参考文章

- https://www.exploit-db.com/exploits/38383/
- http://www.freebuf.com/vuls/99942.html

说明：

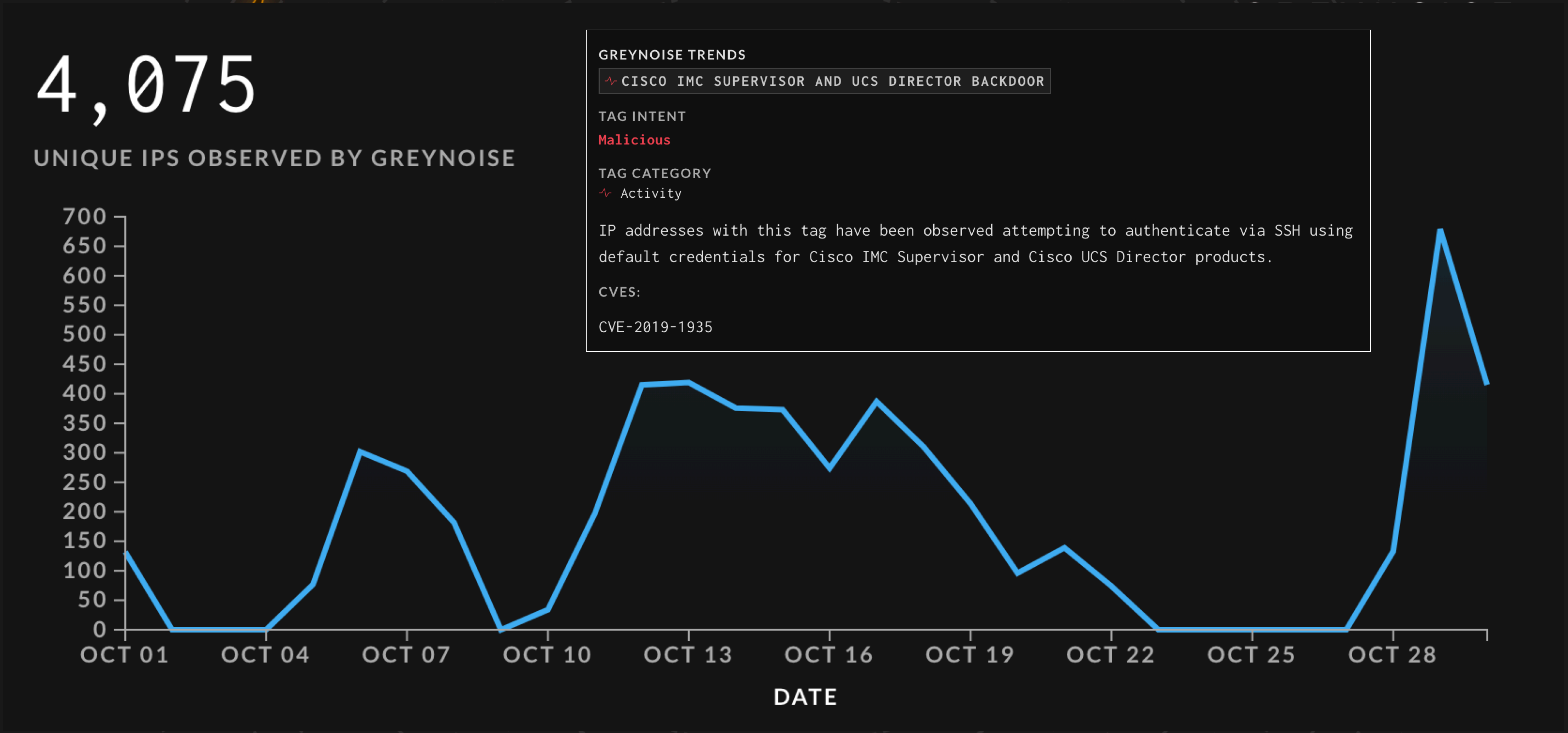
elasticsearch 1.5.1及以前，无需任何配置即可触发该漏洞。之后的新版，配置文件elasticsearch.yml中必须存在`path.repo`，该配置值为一个目录，且该目录必须可写，等于限制了备份仓库的根位置。不配置该值，默认不启动这个功能。

漏洞复现

1. 新建一个仓库

```
PUT /_snapshot/test HTTP/1.1
Host: your-ip:9200
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0
Connection: close
```

https://github.com/vulhub/vulhub/blob/master/elasticsearch/CVE-2015-5531/README.md



4,075

UNIQUE IPS OBSERVED BY GREYNOISE

GREYNOISE TRENDS

CISCO IMC SUPERVISOR AND UCS DIRECTOR BACKDOOR

TAG INTENT

Malicious

TAG CATEGORY

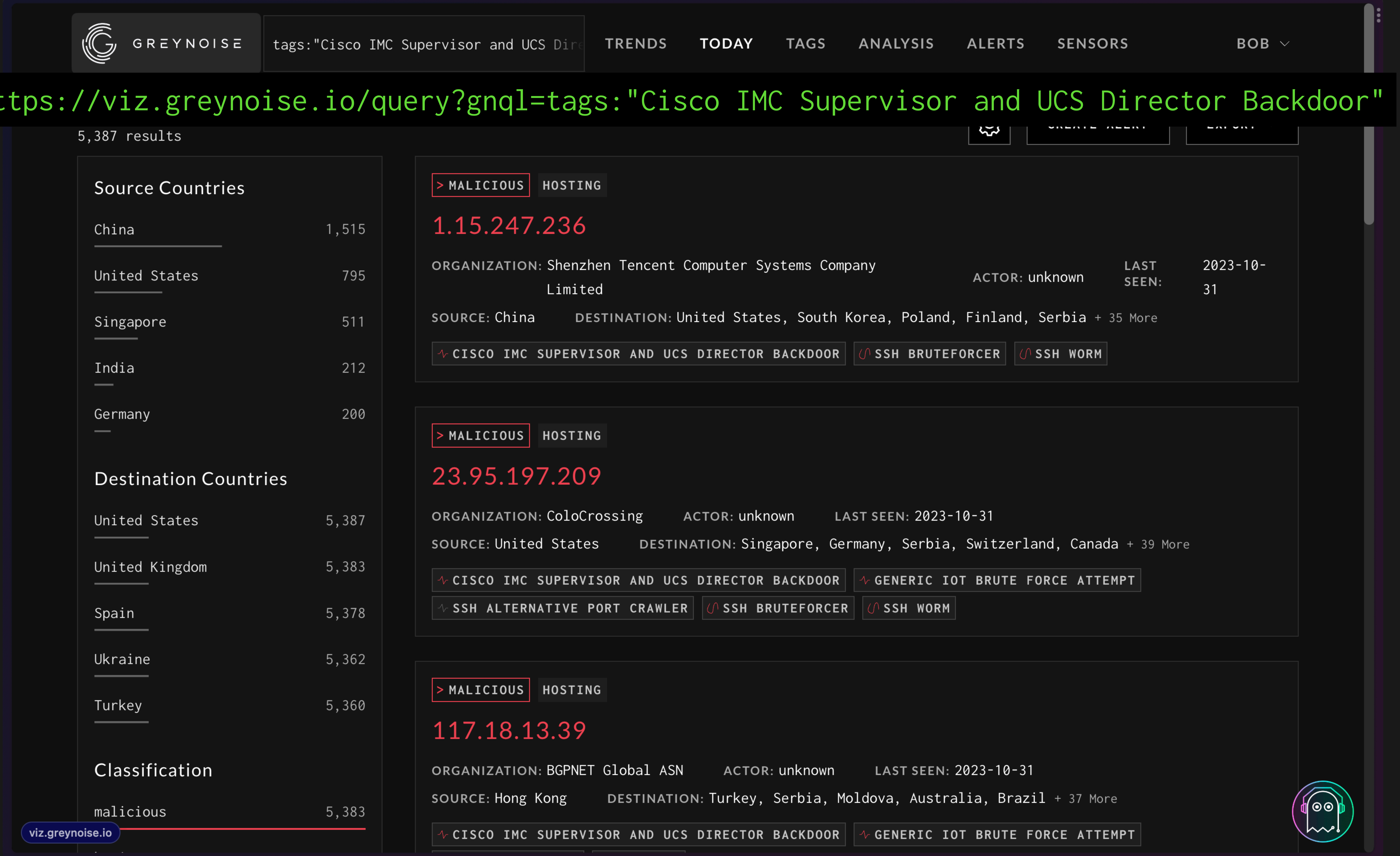
Activity

IP addresses with this tag have been observed attempting to authenticate via SSH using default credentials for Cisco IMC Supervisor and Cisco UCS Director products.

CVES:

CVE-2019-1935

https://viz.greynoise.io/tag/cisco-imc-supervisor-and-ucs-director-backdoor-attempt?days=30



https://viz.greynoise.io/query?gnql=tags:"Cisco IMC Supervisor and UCS Director Backdoor"

5,387 results

Source Countries

China	1,515
United States	795
Singapore	511
India	212
Germany	200

Destination Countries

United States	5,387
United Kingdom	5,383
Spain	5,378
Ukraine	5,362
Turkey	5,360

Classification

malicious	5,383

> MALICIOUS HOSTING

1.15.247.236

ORGANIZATION: Shenzhen Tencent Computer Systems Company Limited ACTOR: unknown LAST SEEN: 2023-10-31

SOURCE: China DESTINATION: United States, South Korea, Poland, Finland, Serbia + 35 More

CISCO IMC SUPERVISOR AND UCS DIRECTOR BACKDOOR | SSH BRUTEFORCER | SSH WORM

> MALICIOUS HOSTING

23.95.197.209

ORGANIZATION: ColoCrossing ACTOR: unknown LAST SEEN: 2023-10-31

SOURCE: United States DESTINATION: Singapore, Germany, Serbia, Switzerland, Canada + 39 More

CISCO IMC SUPERVISOR AND UCS DIRECTOR BACKDOOR | GENERIC IOT BRUTE FORCE ATTEMPT | SSH ALTERNATIVE PORT CRAWLER | SSH BRUTEFORCER | SSH WORM

> MALICIOUS HOSTING

117.18.13.39

ORGANIZATION: BGPNET Global ASN ACTOR: unknown LAST SEEN: 2023-10-31

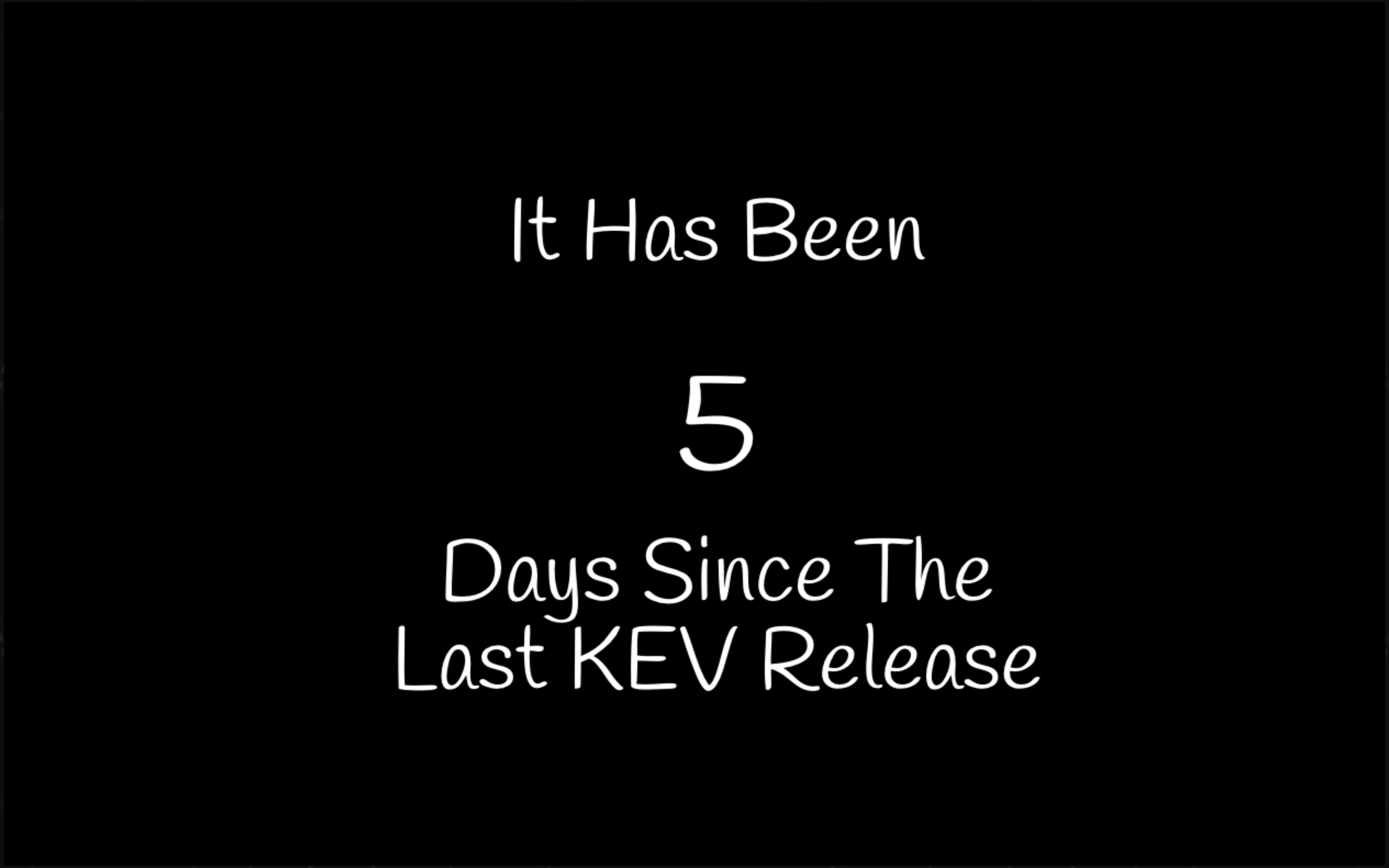
SOURCE: Hong Kong DESTINATION: Turkey, Serbia, Moldova, Australia, Brazil + 37 More

CISCO IMC SUPERVISOR AND UCS DIRECTOR BACKDOOR | GENERIC IOT BRUTE FORCE ATTEMPT

viz.greynoise.io

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

- 🏷 Dell EMC CGi Injection Check
- 🏷 Laravel Telescope Scanner



It Has Been

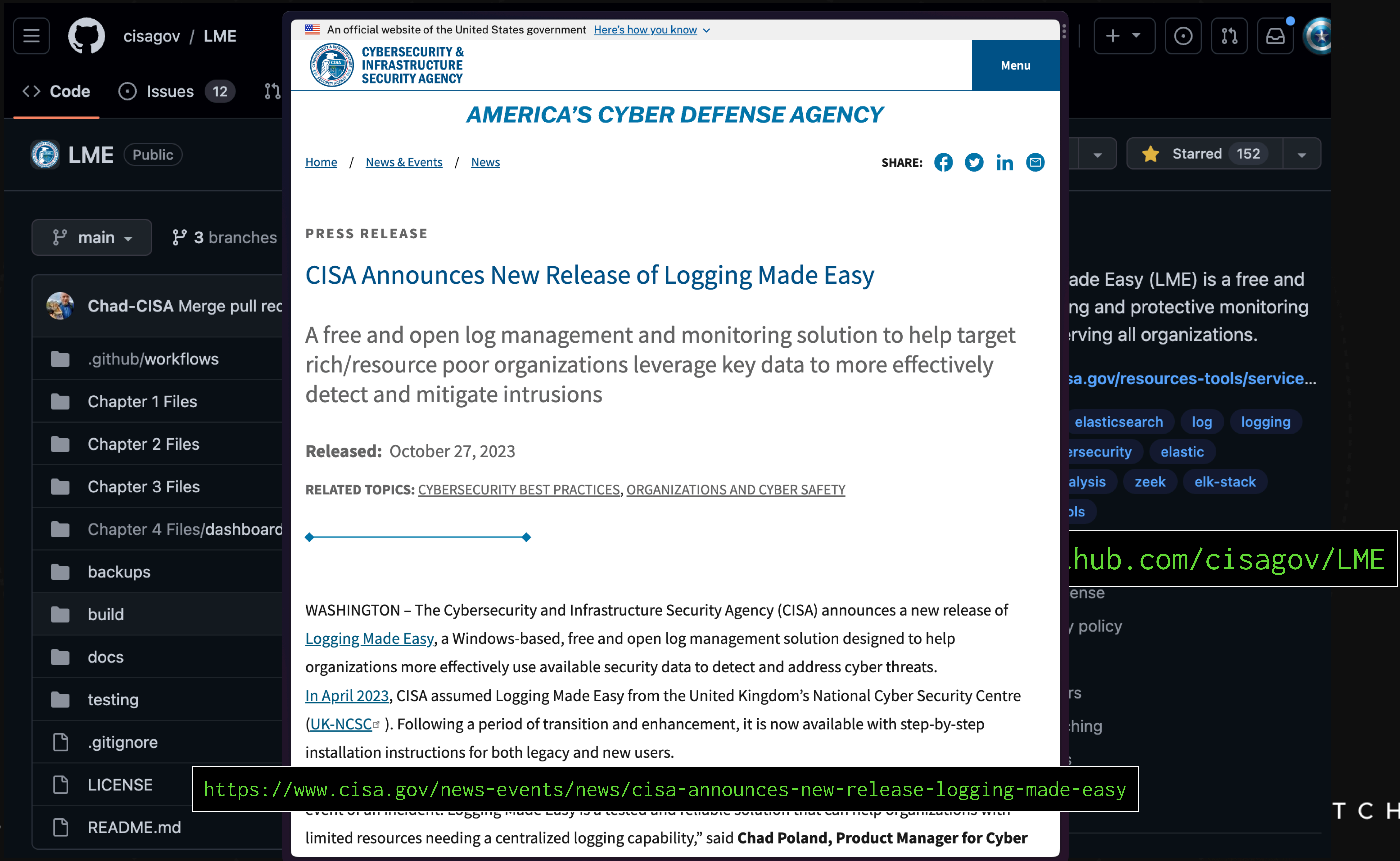
5

Days Since The
Last KEV Release

https://observablehq.com/@greynoise/greynoise-tags https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CVE-2023-5631

Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability


cisagov / LME
Code
Issues 12
LME Public
main
3 branches
Starred 152
Chad-CISA Merge pull req
.github/workflows
Chapter 1 Files
Chapter 2 Files
Chapter 3 Files
Chapter 4 Files/dashboard
backups
build
docs
testing
.gitignore
LICENSE
README.md
ade Easy (LME) is a free and
ng and protective monitoring
erving all organizations.
sa.gov/resources-tools/service...
elasticsearch
log
logging
ersecurity
elastic
alysis
zeek
elk-stack
ols
ense
y policy
rs
hing
An official website of the United States government Here's how you know
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
Menu
AMERICA'S CYBER DEFENSE AGENCY
Home / News & Events / News
SHARE:

PRESS RELEASE

CISA Announces New Release of Logging Made Easy

A free and open log management and monitoring solution to help target rich/resource poor organizations leverage key data to more effectively detect and mitigate intrusions

Released: October 27, 2023

RELATED TOPICS: CYBERSECURITY BEST PRACTICES, ORGANIZATIONS AND CYBER SAFETY

WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA) announces a new release of Logging Made Easy, a Windows-based, free and open log management solution designed to help organizations more effectively use available security data to detect and address cyber threats.

In April 2023, CISA assumed Logging Made Easy from the United Kingdom's National Cyber Security Centre (UK-NCSC). Following a period of transition and enhancement, it is now available with step-by-step installation instructions for both legacy and new users.

limited resources needing a centralized logging capability," said **Chad Poland, Product Manager for Cyber**

hub.com/cisagov/LME

https://www.cisa.gov/news-events/news/cisa-announces-new-release-logging-made-easy

The US Cybersecurity and Infrastructure Security Agency (CISA) is facing potential budget cuts due to its efforts to combat election disinformation, which some lawmakers view as a threat to free speech.

They are being proposed due to CISA's efforts to combat disinformation about US elections, which some lawmakers view as a threat to free speech. Last month, half of House Republicans voted for an amendment to cut funding to CISA by 25%, and Senator Rand Paul (R-KY) has blocked cybersecurity legislation at least 11 times over concerns that CISA and its parent, the US Department of Homeland Security (DHS), are censoring free speech

The cuts could significantly impact CISA's primary responsibilities of defending federal networks and aiding critical infrastructure operators against cyberattacks. Despite its active outreach to private industry, software makers, and cybersecurity firms, and its commitment to helping vulnerable organizations, the proposed cuts could reverse a history of bipartisan budget increases for CISA. The agency is also facing challenges in hiring and retaining cybersecurity professionals, with a 38% understaffing in its Cybersecurity Division as of August 2022

Source: Kamira via Alamy Stock Photo

Storm⚡Watch