

S T O R M ⚡ W A T C H

GREYNOISE



Dateline: 2023-10-03



Following

mle ✨

@mle@infosec.exchange

🧠 security research @ Censys ✨ data science 🏃 runner 🧑 she/her

#infosec / #ml / #cti / #threatIntelligence / #threatResearch / #python /
#psychology / #cognitiveScience / #running / #coffee

Emily
Austin

@mle@infosec.exchange

arepiechartsgood.info

whylime

S T O R M ⚡ W A T C H

GREYNOISE



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.libsyn.com/>

FEMA and FCC Plan Nationwide Emergency Alert Test for Oct. 4, 2023

🌐 English Español

Release Date	Release Number
August 3, 2023	HQ-23-124

<https://www.fema.gov/press-release/20230803/fema-and-fcc-plan-nationwide-emergency-alert-test-oct-4-2023>

Release Date: August 3, 2023

Test Messages Will be Sent to All TVs, Radios and Cell Phones

WASHINGTON -- FEMA, in coordination with the Federal Communications Commission (FCC), will conduct a [nationwide test](#) of the [Emergency Alert System](#) (EAS) and [Wireless Emergency Alerts](#) (WEA) this fall.

The national test will consist of two portions, testing WEA and EAS capabilities. Both tests are scheduled to begin at approximately 2:20 p.m. ET on Wednesday, Oct. 4.

The WEA portion of the test will be directed to all consumer cell phones. This will be the third nationwide test, but the second test to all cellular devices. The test message will display in either English or in Spanish, depending on the language settings of the wireless handset.

The EAS portion of the test will be sent to radios and televisions. This will be the seventh nationwide EAS test.



<https://censys.com/cve-2023-40044/>


BLOG

CVE-2023-40044: A Look at the Critical Ad Hoc Transfer Module Vulnerability in WS_FTP






<https://infosec.exchange/@dangoodin/111139516454103046>

Detail

 **Dan Goodin**
@dangoodin@infosec.exchange





After correcting the improperly scoped libwebp vulnerability on Tuesday -- by submitting a separate CVE and bumping up the severity rating -- Google has now pulled the new CVE and revised the description of the old one.

The moves on both Tuesday and today were completely opaque, meaning Google just made the submissions without announcing or explaining them. The revised CVE also reverts back to older, lower severity rating.

 4  10   

Sep 27, 2023 at 18:40 

 **Dan Goodin** @dangoodin@infosec.exchange 5d
Correction: Google didn't pull the new CVE. Mitre did. Most likely, Mitre agreed with all the critics who blasted Google for creating two CVEs for the same vulnerability.

2  13   

After correcting the improperly scoped libwebp vulnerability on Tuesday -- by submitting a separate CVE and bumping up the severity rating -- Google has now pulled the new CVE and revised the description of the old one.

The moves on both Tuesday and today were completely opaque, meaning Google just made the submissions without announcing or explaining them. The revised CVE also reverts back to older, lower severity rating.





Dewey Ritten (taylor's version) 

@deweyritten@infosec.exchange

So a lot of people who are in unstable, abusive, and/or periodically violent living situations keep cell phones hidden for emergencies.

If you know anyone in such a situation, make sure they know about FEMA's testing of its Wireless Emergency Alert (WEA) system next Wednesday (10/4). This test will bypass the phone's silencing features. To keep the phone quiet during this alert, it has to be completely powered down.

<https://infosec.exchange/@deweyritten/111149733617347257>



<https://www.cisa.gov/news-events/news/transforming-vulnerability-management-cisa-adds-oasis-csaf-20-standard-ics-advisories>

BLOG

Transforming Vulnerability Management: CISA Adds OASIS CSAF 2.0 Standard to ICS Advisories

Released: September 29, 2023

By Lindsey Cerkovnik, Chief of Vulnerability Response and Coordination, and Daniel Larson, Justin Murphy, and Brandon Tarr

RELATED TOPICS: [CYBERSECURITY BEST PRACTICES](#), [CYBER THREATS AND ADVISORIES](#)



In our pursuit to “[transform the vulnerability management landscape](#),” CISA is excited to announce that our security advisories for **Industrial Control Systems (ICS)**, **Operational Technology (OT)**, and Medical Devices now include the OASIS Common Security Advisory Framework (CSAF) Version 2.0 standard.

In the current risk environment, organizations are challenged to manage the growing number and complexity of new vulnerabilities. A critical step in helping organizations achieve better efficiency in triaging and prioritizing vulnerability management efforts is introducing greater automation into the ecosystem. CSAF supports automation

mstrad Merge pull request #7 from cisagov/working	5668593 3 days ago	🕒 28 commits
📁 csaf_files/OT/white	URL fix on ICSA-22-277-02	3 days ago
📄 README.md	Added reference to provider metadata	last month

README.md

CISA CSAF

CISA CSAF (Common Security Advisory Framework) Security Advisory Repository

OASIS Standard

CSAF Security Advisory files were designed following the standard published by [OASIS Open](#).

Contact

Please submit issues to the Issues Tracker of the CSAF repository with any comments or questions.

CISA CSAF Trusted Provider

About

CISA CSAF ICSA Security Advisories

- 📖 Readme
- 🔗 Security policy
- 📈 Activity
- ★ 6 stars
- 👁 8 watching
- 🍴 2 forks

Report repository

Releases

No releases published

Packages

No packages published

Improper Control of a Resource Through its Lifetime

CWE-125 CWE-787 CWE-121

CWE-416 CWE-400 CWE-200 CWE-120

CWE-119 CWE-427 CWE-434 CWE-502 CWE-611

CWE-522 CWE-843 CWE-822 CWE-312 CWE-668 CWE-415

CWE-122 CWE-276 CWE-732

CWE-22 CWE-23 CWE-256

CWE-94 CWE-824 CWE-770

Improper Access Control

CWE-287 CWE-306 CWE-798

CWE-269 CWE-276 CWE-256 CWE-295 CWE-259

CWE-321 CWE-285

CWE-522 CWE-288

CWE-732

Improper Neutralization

CWE-20 CWE-79

CWE-89 CWE-77 CWE-94 CWE-88

CWE-78

Protection Mechanism Failure

CWE-798 CWE-326 CWE-321

CWE-319 CWE-311 CWE-327 CWE-345

CWE-352 CWE-330 CWE-259

Improper Adherence to Coding Standards

CWE-798 CWE-476

CWE-321 CWE-259

Improper Check or Handling of Exceptional Conditions

CWE-476

CWE-362 CWE-307

CWE-190

Improper Control of a Resource Through its Lifetime

CWE-125

CWE-787

CWE-121

Improper Access Control

CWE-287

CWE-306

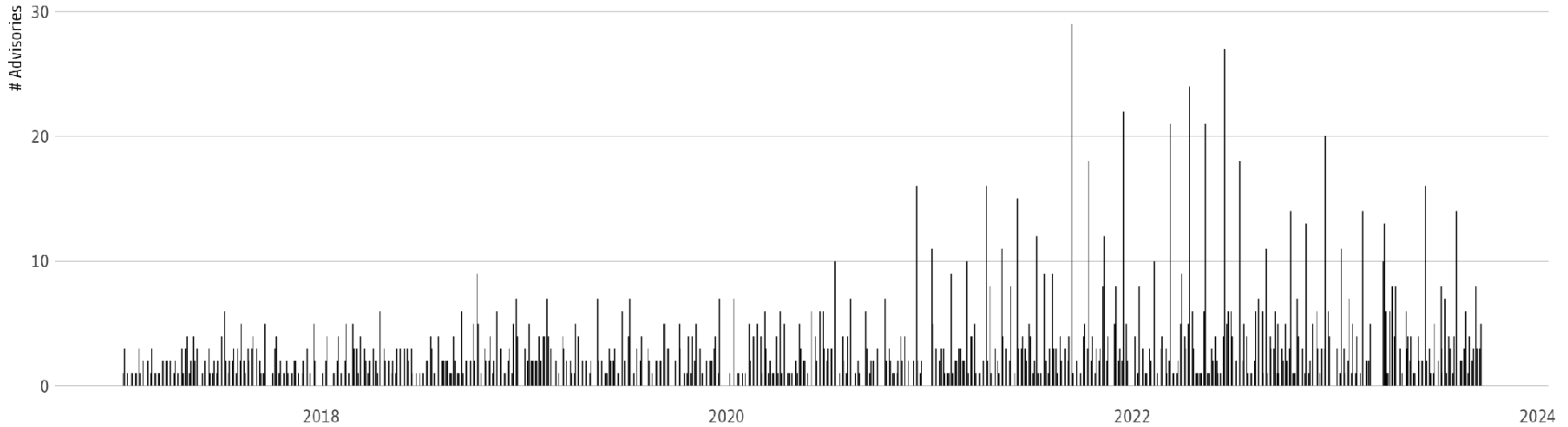
CWE-798

Improper Neutralization

CWE-20

CWE-79

CISA ICS/OT Advisories



CWE-22

CWE-824

CWE-94

CWE-770

CWE-352

CWE-259

CWE-259

CWE-307

CWE-307



Healthcare

FDA's Refuse to Accept Policy is Here

George V. Hulme / Sep 28, 2023

<https://nexusconnect.io/articles/fdas-refuse-to-accept-policy-is-here>

Starting Oct.1, significant changes are going into effect for medical device manufacturers—and medical device cybersecurity experts have mixed opinions on whether device makers are ready for the change.

The **FDA's "Refuse to Accept" policy** relates to the FDA's review of medical devices and their premarket submission notification, known as the 510(k) submission process (named after the submission form). Under the new Refuse to Accept policy, the FDA will automatically begin rejecting premarket medical device submissions if they fail to meet the FDA's expected description of device security measures, including security controls, handling vulnerability disclosure with security researchers, and a software bill of materials (SBOM).

Share



Featured Articles

[Considerations for Medical Device](#)

Starting Oct.1, significant changes are going into effect for medical device manufacturers—and medical device cybersecurity experts have mixed opinions on whether device makers are ready for the change.

The FDA's "Refuse to Accept" policy relates to the FDA's review of medical devices and their premarket submission notification, known as the 510(k) submission process (named after the submission form). Under the new Refuse to Accept policy, the FDA will automatically begin rejecting premarket medical device submissions if they fail to meet the FDA's expected description of device security measures, including security controls, handling vulnerability disclosure with security researchers, and a software bill of materials (SBOM).

🦋 @awpiii.bsky.social

Bill Pelletier, an embedded systems security architect at a medical device and software maker based in the northeast U.S., says device makers should already be quite prepared for the updated policy. "It should be no surprise to any MDM when/if their submissions are summarily returned for rework due to lack of compliance to section 524B of the FD&C Act (Omnibus Appropriations)," he says.

Pelletier and others say the new policy is simply transferring what traditionally has occurred between the FDA and the MDM post-submission back to the MDM for pre-submission completion. "It (hopefully) removes the inefficiencies of that back-and-forth negotiation and rework that occurred when MDMs submitted less-than complete (or accurate) submissions for cyber devices," Pelletier says.

https://www.csoonline.com/article/653460/dhs-unveils-one-common-platform-for-reporting-cyber-incidents.html

Home • Security • DHS unveils one common platform for reporting cyber incidents

by Cynthia Brumfield
Contributing Writer

in [social icons]

DHS unveils one common platform for reporting cyber incidents

News Analysis

Sep 25, 2023 • 10 mins

Government | Incident Response | Regulation

Ahead of CISA cyber incident reporting regulations, DHS issued a report on harmonizing 52 cyber incident reporting requirements, presenting a model common reporting platform that could encompass them all.



Related content

News

Multibillion-dollar cybersecurity training market fails to fix the supply-demand imbalance

Despite money pouring into programs around the world, training organizations have not managed to ensure employment for professionals, while entry-level professionals are finding it hard to land a job

By Gemma Corneil

in

[social icon]

>

ADVISORY DETAILS

<https://www.zerodayinitiative.com/advisories/ZDI-23-1469/>

September 27th, 2023

(0Day) Exim AUTH Out-Of-Bounds Write Remote Code Execution Vulnerability

[ZDI-23-1469](#)

[ZDI-CAN-17434](#)

CVE ID

[CVE-2023-42115](#)

CVSS SCORE

9.8, (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

AFFECTED VENDORS

[Exim](#)

AFFECTED PRODUCTS

[Exim](#)

VULNERABILITY DETAILS

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Exim. Authentication is not required to exploit this vulnerability.

The specific flaw exists within the smtp service, which listens on TCP port 25 by default. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of a buffer. An attacker can leverage this vulnerability to execute code in the context of the service account.

ADDITIONAL DETAILS

06/06/22 – ZDI requested a PSIRT contact.

Six 0-Day exploits were filed against Exim.

None of these issues is related to transport security (TLS) enablement.

- * 3 of them are related to SPA/NTLM, and EXTERNAL auth. If you do not use SPA/NTLM, or EXTERNAL authentication, you're not affected. These issues are fixed.
- * One issue is related to data received from a proxy-protocol proxy. If you do not use a proxy in front of Exim, you're not affected. If your proxy is trustworthy, you're not affected. **We're working on a fix.** 🙄
- * One is related to libspf2. If you do not use the `spf` lookup type or the `spf` ACL condition, you are not affected.
- * The last one is related to DNS lookups. If you use a trustworthy resolver (which does validation of the data it receives), you're not affected. We're working on a fix.


<https://www.404media.co/260-million-ai-company-releases-chatbot-that-gives-detailed-instructions-on-murder-ethnic-cleansing/>

NEWS

260 Million AI

MURDERGPT

INSTRUCTIONS ON Murder, Ethnic Cleansing

 EMANUEL MAIBERG · SEP 29, 2023 AT 11:20 AM

Mistral, an AI company founded by former Google and Meta alums pushed an “unmoderated” model into the world that will readily tell users how to kill their wives or restore Jim Crow-style discrimination.

CSS



GREYNOISE
LABS

Script

Images
/favicon.ico

Misc

/%5ccgi-bin/get_status.cgi

google.com:443

www.google.com:443

133.21-

..98.7-

1.90.207-

1.41.08.247-

1.244.165-

185.36.81-

1.235.24-

1.98.58-

1.210.31-

03.210-

1.5.194-

28.232-

62.197-

49.1-

68.69.184-

17.149-

54.51-

128.6.117-6-

Sift™ is in the GreyNoise Early Access Program until December 31, 2023. For continued use or feedback please email sift@greynoise.io.



[Explore Our Data](#)

[GN Labs](#)

[GN Labs APIs](#)

[About GreyNoise](#)

[Triage](#)

[Explore](#)

[About Sift™](#)

<https://sift.labs.greynoise.io/>

September 2023 ▼

2023-09-25

2023-09-24

2023-09-23

2023-09-22

2023-09-21

2023-09-20

2023-09-19

2023-09-18

Prev

Next

Day's 📅

Day's IP/📄 Metadata

Sift run: 2023-09-25 | Record 1 / 22 | UUID: f81d7ad1-65f1-40d9-b4e7-0945b615dafb

URL-based SQL Injection Identified

SQL Injection

🔔 8

📊 0.8

Active Users

Data Manipulation

Database Exploit

GET Request

ID Extraction

Input Validation

SQL Injection

URL-based Injection

Unauthorized Access

Web Application Vulnerability

Analysis

The HTTP request shared carries a SQL injection payload in the URL parameters, using UNION SELECT SQL Injection technique to extract data from 'DOMAINS' and 'users' table of an underlying SGMSDB database. This payload can be detrimental, especially if they are carrying privileged account IDs or session IDs, thus giving the attacker an elevated privilege access to other user(s) data. The payload's attempt towards active users signifies that the attacker is targetting potentially active accounts, thereby increasing the impact. This attack is marked as URL Based or 'GET' SQL injection and could possibly lead to unauthorized access, data exfiltration, and data manipulation or deletion. The exploit ultimately indicates the need for input validation and appropriate use of prepared statements or stored procedures in database queries.

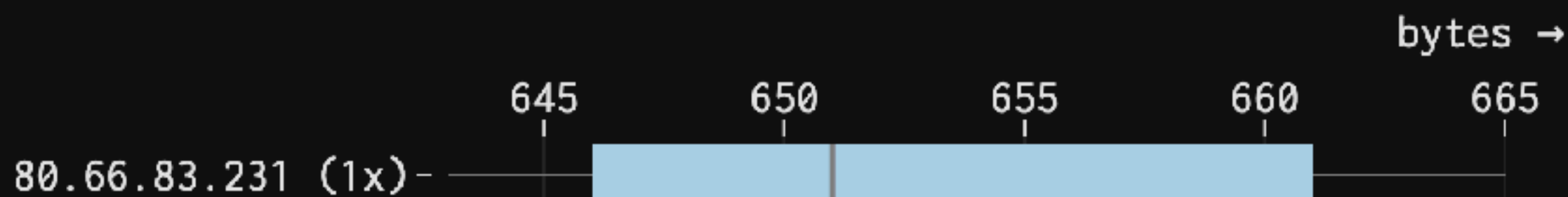
Tag Suricata

```
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"SQLi Attack Detected"; content:"UNION SELECT"; content:"ACTIVE = 1"; http_uri; classtype:web-application-attack; sid:1000201; rev:1;)
```

IP Payload Volume Distribution

Total samples: 126

Found in # other records today



[Click to open IP addresses in the GreyNoise Visualizer](#)

Analysis

The HTTP request shared carries a SQL injection payload in the URL parameters, using UNION SELECT SQL Injection technique to extract data from 'DOMAINS' and 'users' table of an underlying SGMSDB database. This payload can be detrimental, especially if they are carrying privileged account IDs or session IDs, thus giving the attacker an elevated privilege access to other user(s) data. The payload's attempt towards active users signifies that the attacker is targetting potentially active accounts, thereby increasing the impact. This attack is marked as URL Based or 'GET' SQL injection and could possibly lead to unauthorized access, data exfiltration, and data manipulation or deletion. The exploit ultimately indicates the need for input validation and appropriate use of prepared statements or stored procedures in database queries.

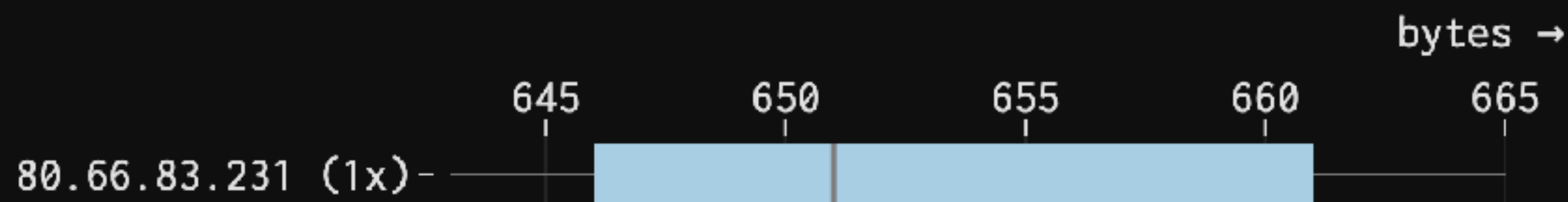
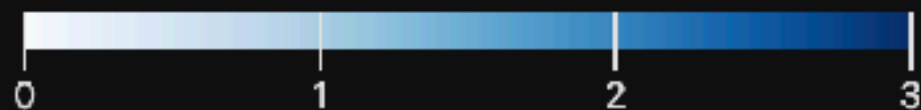
Tag Suricata

```
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"SQLi Attack Detected"; content:"UNION SELECT"; content:"ACTIVE = 1"; http_uri; classtype:web-application-attack; sid:1000201; rev:1;)
```

IP Payload Volume Distribution

Total samples: 126

Found in # other records today



Click to open IP addresses in the GreyNoise Visualizer

Existing IP Tags

Tap a tag to highlight which IPs have been associated with that activity.
Hold down Alt/Option key and tap to open that Tag in the GreyNoise Visualizer.

- SonicWall SQL Injection Attempt
- TLS/SSL Crawler
- Web Crawler

Reload Database

Check & Update Database

Download CSV

Report Date ▲	IP Address ▲	ASN ▲	Tag Count ▲	Attack Types ▲	Threat Score ▲	Title ▲	Confidence ▲
2023-09-22	103.68.61.97	AS133380	87	SQL Injection	9	Potential SQL Inj...	0.9
2023-09-22	103.68.61.97	AS133380	87	Command Injection	9	Potential Command...	0.8
2023-09-22	35.234.59.152	AS396982	226		8	Possible Unprotec...	0.8
2023-09-22	35.234.59.152	AS396982	225	File upload,Cross...	8	Potentially Malic...	0.85
2023-09-22	103.68.61.97	AS133380	87	Server-side Templ...	8	Potential Server-...	0.85
2023-09-22	35.234.59.152	AS396982	226	Path Traversal at...	8	[Potential Exploi...	0.85
2023-09-22	35.234.59.152	AS396982	226	SQL Injection	8	Potential SQL Inj...	0.85
2023-09-22	103.68.61.97	AS133380	87	Cross-site Script...	8	Potential Cross-S...	0.9
2023-09-22	103.68.61.97	AS133380	87	Code Injection	8	Suspicious HTTP P...	0.85
2023-09-22	103.68.61.97	AS133380	87	Configuration exp...	8	Potential ASHX Ha...	0.85

761 unique IPs | 35 unique IPs w/o 🚩 | 232 unique ASNs | 0 unique ASNs w/o 🚩

- 📁 Progress WS_FTP Server CVE-2023-40044 RCE Attempt
- 📁 Progress WS_FTP Server Scanner
- 📁 JetBrains TeamCity Authentication Bypass Attempt
- 📁 Qlik Sense RCE Attempt
- 📁 Qlik Sense HTTP Tunneling Attempt
- 📁 Qlik Sense Auth Bypass Attempt
- 📁 GeoServer Scanner

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

3 DAYS

10 DAYS

• 30 DAYS

September 03, 2023 - October 03, 2023

74

UNIQUE

GREYNOISE TRENDS

📈 JETBRAINS TEAMCITY AUTHENTICATION BYPASS ATTEMPT

TAG INTENT

Malicious

TAG CATEGORY

📈 Activity

IP addresses with this tag have been observed attempting to exploit CVE-2023-42793, an authentication bypass vulnerability in JetBrains TeamCity.



<https://viz.greynoise.io/tag/jetbrains-teamcity-authentication-bypass-attempt?days=30>

3 DAYS

10 DAYS

• 30 DAYS

September 03, 2023 - October 03, 2023

589

UNIQUE IPS

GREYNOISE TRENDS

📈 GEOSERVER SCANNER

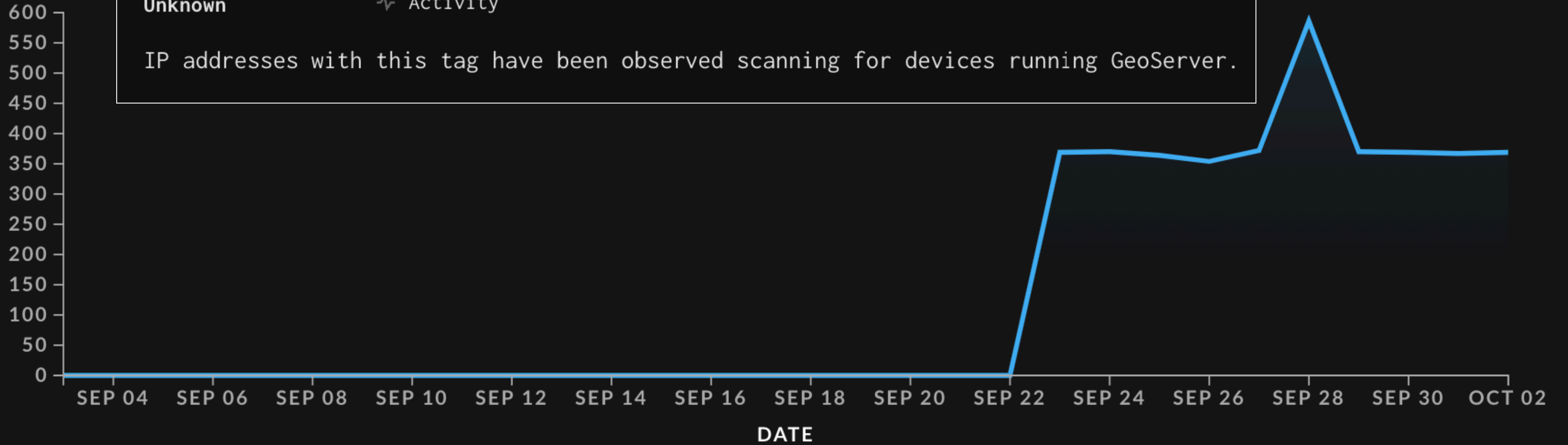
TAG INTENT

Unknown

TAG CATEGORY

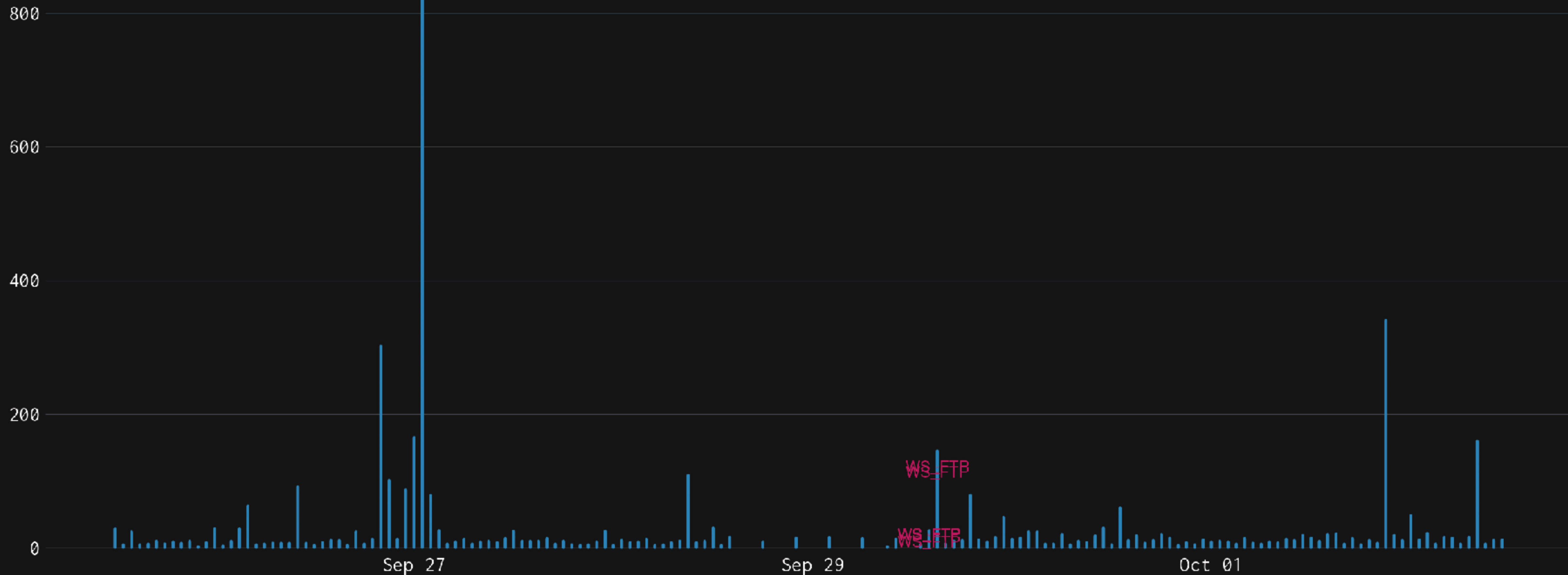
📈 Activity

IP addresses with this tag have been observed scanning for devices running GeoServer.



<https://viz.greynoise.io/tag/geoserver-scanner?days=30>

Remy's Sensor HTTP Events



S

> UNKNOWN EDUCATION

192.42.116.173

ORGANIZATION SURF B.V. ACTOR unknown Not Spoofable [?]

0 similar IPs

FIRST SEEN 2023-02-05 LAST SEEN 2023-09-12

COUNTRY Netherlands REGION Utrecht CITY Nieuwegein ASN AS1101

DESTINATIONS United States, Ukraine

OS FreeBSD RDNS 21.tor-exit.nothingtohide.nl

> TOR



Observed Activity

Shows the ports & protocols that this IP scanned, along with the paths that this IP requested. In addition, fingerprints of the SSH & TLS negotiation between this IP and the GreyNoise sensor are shown.

SUMMARY

TIMELINE

Ports Scanned [?]

PORT	PROTOCOL
80	TCP
443	TCP

Web Requests [?]

PATHS

/

USER-AGENTS

Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; W:

JA3 Fingerprints [?]

FINGERPRINT	PORT
No fingerprint data detected.	-

HASSH Fingerprints [?]

FINGERPRINT	PORT
No fingerprint data detected.	-

Tags [?]

CARRIES HTTP REFERER

WEB CRAWLER



1



> UNKNOWN MOBILE

192.42.116.198

ORGANIZATION SURF B.V. ACTOR unknown Not Spoofable [?]

0 similar IPs

FIRST SEEN 2022-12-20 LAST SEEN 2023-10-01

COUNTRY Netherlands REGION Utrecht CITY Nieuwegein ASN AS1101

DESTINATIONS United Kingdom, Indonesia, United States

OS FreeBSD RDNS 8.tor-exit.nothingtohide.nl

> TOR



Observed Activity

Shows the ports & protocols that this IP scanned, along with the paths that this IP requested. In addition, fingerprints of the SSH & TLS negotiation between this IP and the GreyNoise sensor are shown.

SUMMARY

TIMELINE

Ports Scanned [?]

PORT	PROTOCOL
80	TCP
443	TCP

Web Requests [?]

PATHS

/wp-content/plugins/woocommerce/readme.txt

/

USER-AGENTS

Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.1

Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101

Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit,

JA3 Fingerprints [?]

FINGERPRINT	PORT
19e29534fd49dd27d09234e639c4057e	443
db687c576d7ee0017b289fc05e0f8574	443
23e59e324a91b1cb77fd83105093ea85	443

Tags [?]

TLS/SSL CRAWLER

WEB CRAWLER



1



SUMMARY

TIMELINE

07/04/23 - 10/01/23

Past 90 days

JULY

AUGUST

S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	01	02	03	04	05	06	07	08	09	10

Classification

Unknown

Tags

TLS/SSL Crawler

Python Requests Cli...

Carries HTTP Referer

Web Crawler



It Has Been

1

Days Since The
Last KEV Release



[\(CVE-2023-5217\)](#) Chrome libvpx

[\(CVE-2018-14667\)](#) JBoss RichFaces Framework

S T O R M ⚡ W A T C H

GREYNOISE



Dateline: 2023-10-03