STORM WATCH

CYBERSECURITY NEWS

Dateline: 2024-08-13

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


paloalto
CyberRisk
Collaborative
Happy Hour
Presented by:
paloalto
NETWORKS
CyberRisk
Collaborative
paloalto

STORM WATCH

CYBERSECURITY NEWS

CYBERSIDE CHAT

Pump Control

System Setpoints

Local Overview

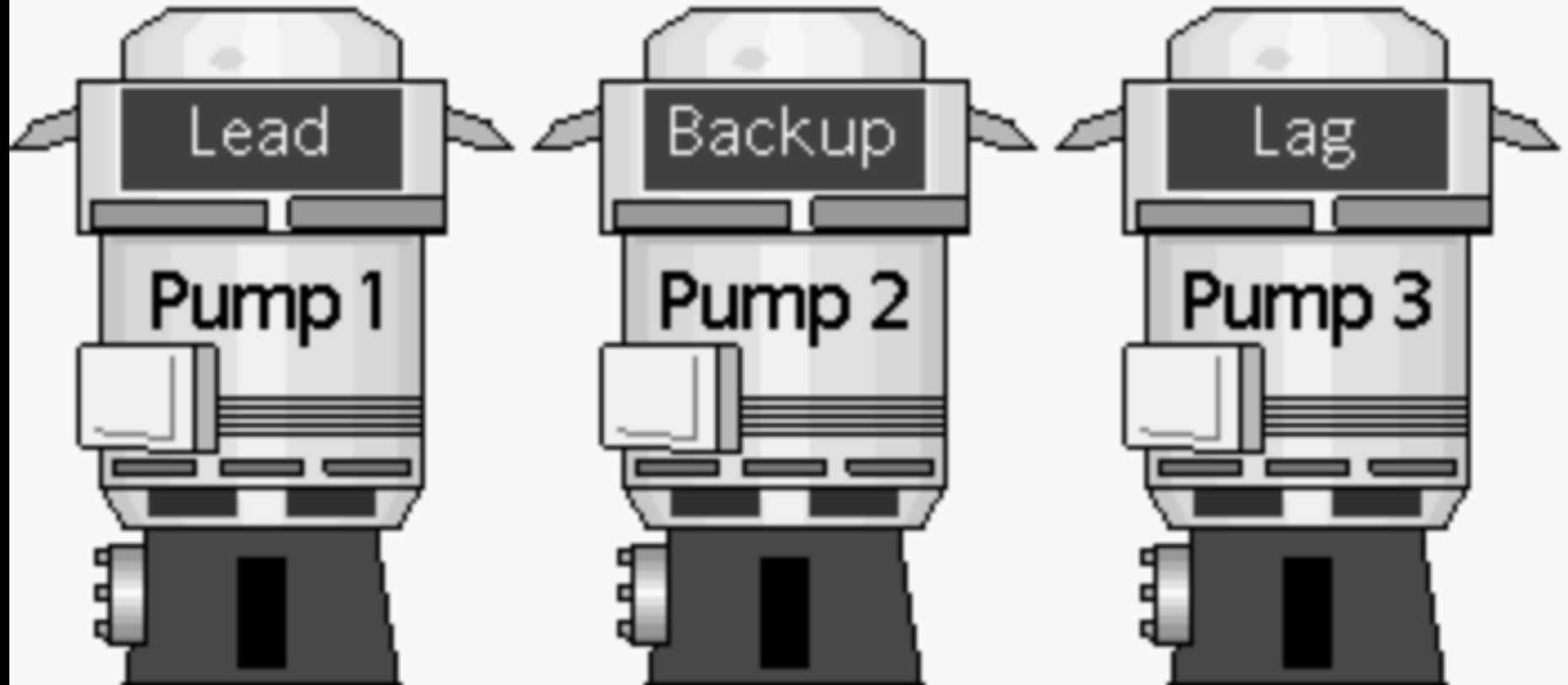
Alarms

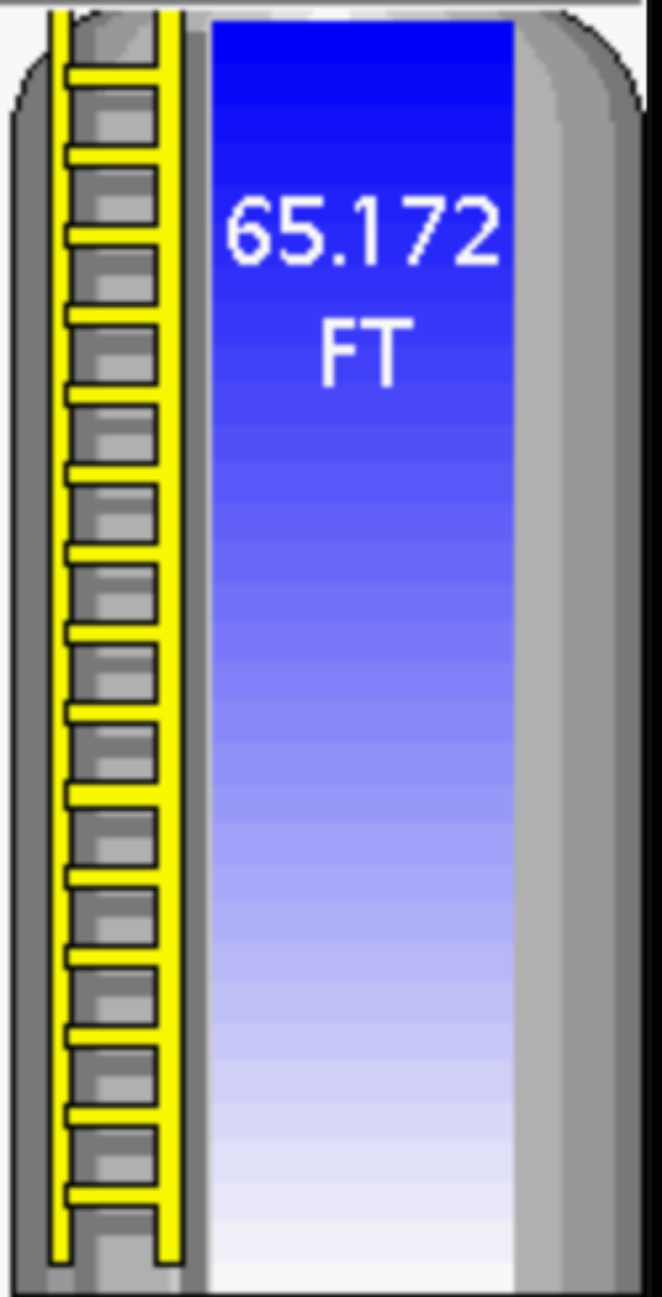
Battery 13.993

Remote Enabled

Offline

Remote Enabled





https://censys.com/research-report-internet-connected-industrial-control-systems-part-one/

censys

BLOGS

Research Report: Internet-Connected Industrial Control Systems (Part One)

STORM WATCH

CYBERSECURITY NEWS

CYBER SPOTLIGHT

VOLEXITY

THREAT INTELLIGENCE

StormBamboo Compromises ISP to Abuse Insecure Software Update Mechanisms

https://www.volexity.com/blog/2024/08/02/stormbamboo-compromises-isp-to-abuse-insecure-software-update-mechanisms/

- StormBamboo compromised an ISP's DNS infrastructure to alter DNS query responses for specific domains.
- This allowed them to redirect traffic for automatic software updates to attacker-controlled servers.
- The attackers targeted software with insecure update mechanisms, particularly those using HTTP instead of HTTPS.
- DNS records were poisoned to resolve to an attacker-controlled server in Hong Kong.
- After compromising systems, StormBamboo deployed a malicious Chrome extension called RELOADEXT.
- This attack demonstrates the risks of using insecure update mechanisms and the potential for widespread compromise through ISP-level attacks.

STORM WATCH

CYBERSECURITY NEWS

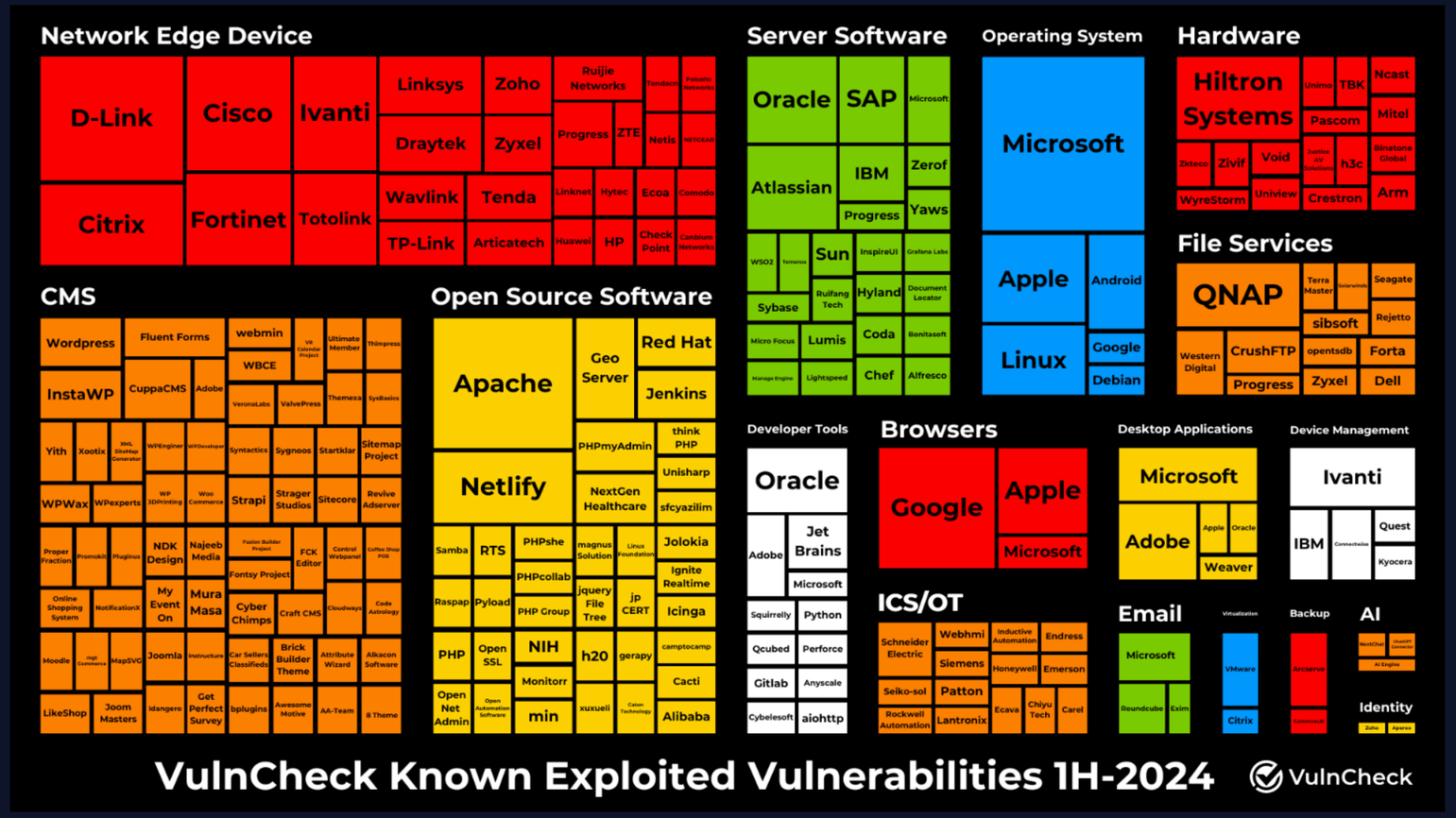
SHAMELESS SELF-PROMOTION

August 5, 2024

State of Exploitation - A Peek into 1H-2024 Vulnerability Exploitation

Patrick Garrity
in/patrickmgarrity/

https://vulncheck.com/blog/state-of-exploitation-1h-2024

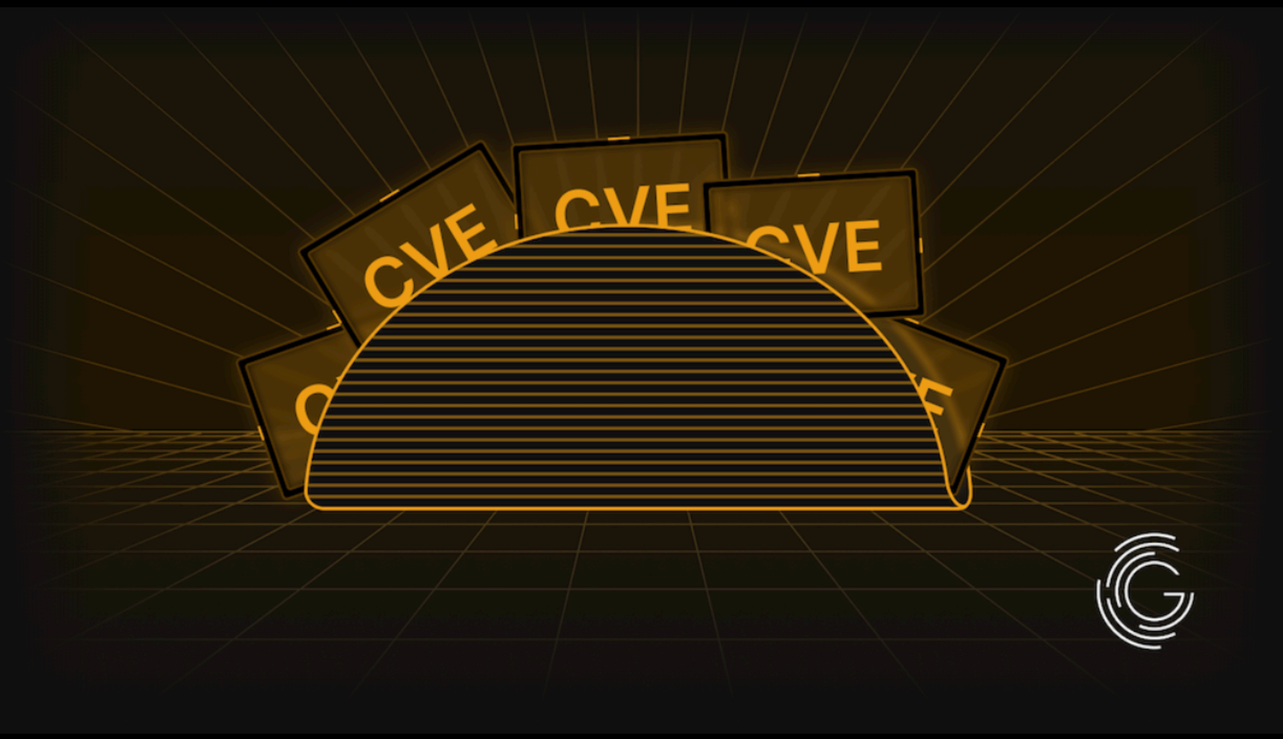


https://www.greynoise.io/blog/the-tortilla-test-ensuring-your-vulnerability-intelligence-is-always-fresh

PRODUCT COMPANY

The Tortilla Test: Ensuring Your Vulnerability Intelligence is Always Fresh

Corey Bodzin | August 1, 2024



KEY CAPABILITIES

Prioritize critical patches by understanding active exploitation trends

Dynamically block malicious IPs mass scanning for a specific vulnerability

Monitor CVEs and get alerted when it's being actively exploited

Search for IPs that may have already breached your perimeter

https://www.greynoise.io/products/vulnerability-management-teams

CVE-2021-44228

Apache Log4j2 Remote Code Execution Vulnerability

In-the-wild activity happening now

GreyNoise has observed IPs scanning or attempting to exploit CVE-2021-44228 in the past 24 hours.

RECOMMENDED ACTION

Block IPs

The endpoint below returns a dynamic list of IPs observed performing exploitation or reconnaissance activity against CVE-2021-44228. Add it to your firewall to block known IPs targeting CVE-2021-44228 in the wild.

```
https://api.greynoise.io/v3/tags/80592a05-bbd6-4813-836d-9ef9f822e951/ips?format=txt&token=pgsJpFPQfc
```

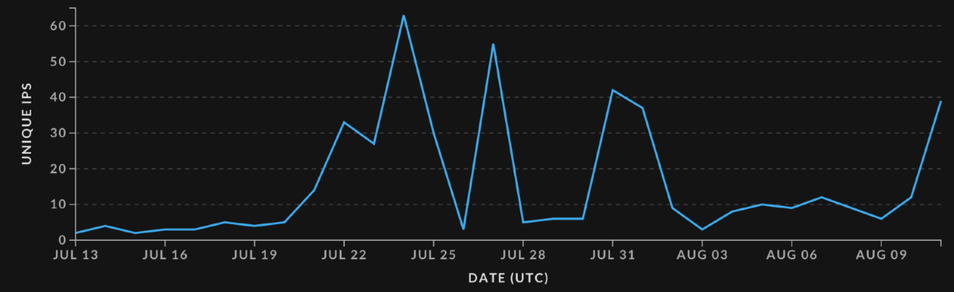
24 HOURS | 10 DAYS | •30 DAYS | July 13, 2024 - August 11, 2024 (UTC)

Unique IPs Observed

Last 30 days

TAGS TRACKING THIS CVE

APACHE LOG4J RCE ATTEMPT



	PAST 1 DAY	PAST 10 DAYS	PAST 30 DAYS
Threat IPs observed [?]	166	200	260
Benign IPs observed [?]	0	0	0

Get in-the-wild CVE data in the platforms you use every day.

splunk> | CORTEX XSOAR | Nucleus

View Integrations | View API Documentation

334 Observed IPs →

VULNERABILITY DESCRIPTION

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in…

[+] SHOW MORE

VENDOR

Apache

PRODUCT

Log4j2

CVSS (VERSION 3.1)

10

EPSS

97% probability of exploitation in the next 30 days

EXPLOITS AVAILABLE

109 (first known exploit published 2021-12-05)

REPORTED EXPLOITATION ACVTIVITY

Threat Actors	33
Botnets	8

CVE-2021-44228

Apache Log4j2 Remote Code Execution Vulnerability

In-the-wild activity happening now

GreyNoise has observed IPs scanning or attempting to exploit CVE-2021-44228 in the past 24 hours.

RECOMMENDED ACTION

Block IPs

The endpoint below returns a dynamic list of IPs observed performing exploitation or reconnaissance activity against CVE-2021-44228. Add it to your firewall to block known IPs targeting CVE-2021-44228 in the wild.

```
https://api.greynoise.io/v3/tags/80592a05-bbd6-4813-836d-9ef9f822e951/ips?format=txt&token=pgsJpFPQfc
```

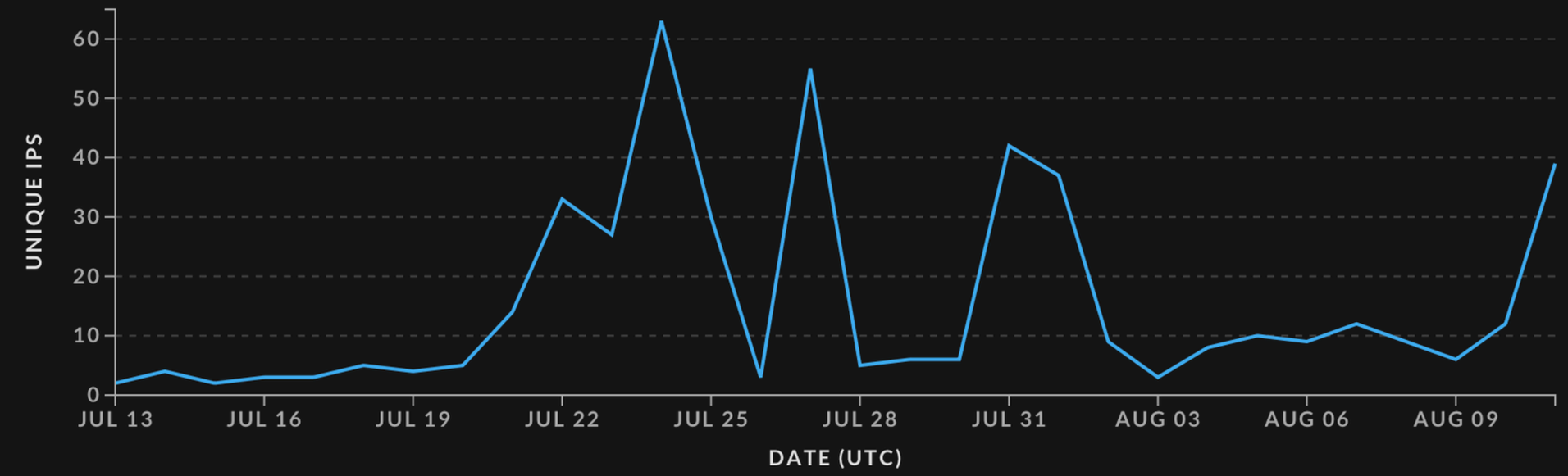
24 HOURS | 10 DAYS | • 30 DAYS | July 13, 2024 - August 11, 2024 (UTC)

Unique IPs Observed

Last 30 days

TAGS TRACKING THIS CVE

APACHE LOG4J RCE ATTEMPT



	PAST 1 DAY	PAST 10 DAYS	PAST 30 DAYS
Threat IPs observed [?]	166	200	260
Benign IPs observed [?]	0	0	0

334 Observed IPs →

VULNERABILITY DESCRIPTION

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in…

[+] SHOW MORE

VENDOR

Apache

PRODUCT

Log4j2

CVSS (VERSION 3.1)

10

EPSS

97% probability of exploitation in the next 30 days

EXPLOITS AVAILABLE

109 (first known exploit published 2021-12-05)

REPORTED EXPLOITATION ACVTIVITY

Threat Actors	33
Botnets	8

STORM WATCH

CYBERSECURITY NEWS

TAG ROUND-UP

GreyNoise Trends

APACHE OFBIZ CVE-2024-32113 PATH TRAVERSAL ATTEMPT

INTENTION
MALICIOUS

CATEGORY
Activity

CVES
CVE-2024-32113

IP addresses with this tag have been observed attempting to exploit CVE-2024-32113, which is a path-traversal vulnerability in Apache OFBiz that can easily be used for remote code execution.

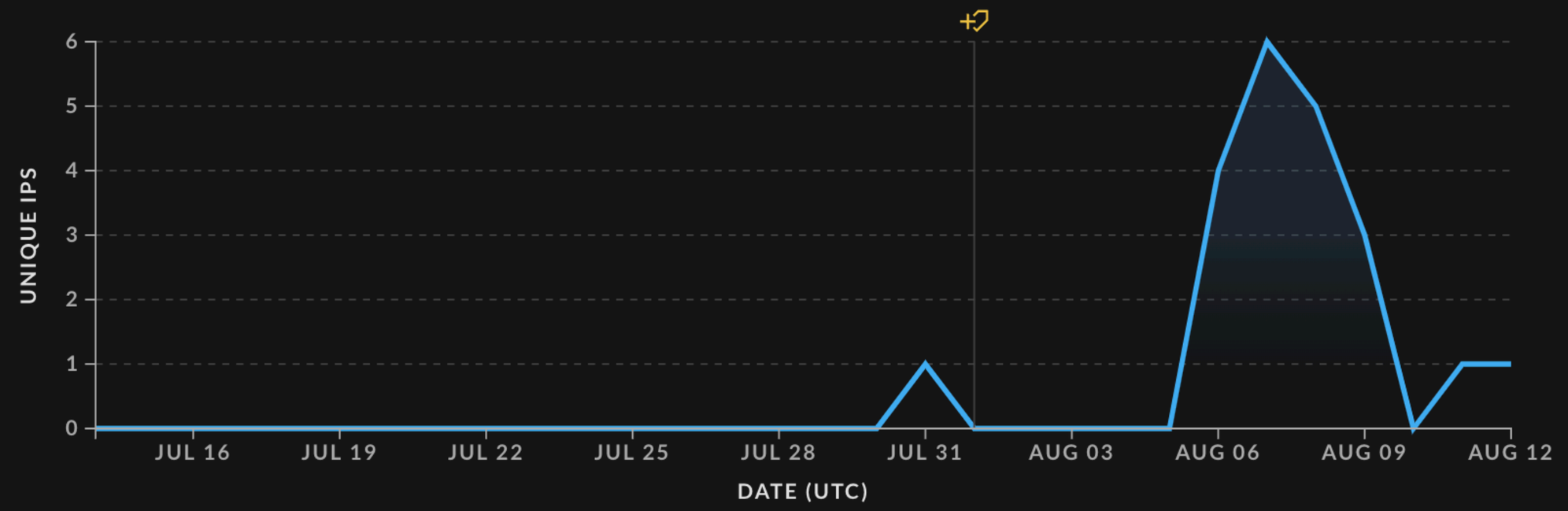
24 HOURS | 10 DAYS | 30 DAYS

July 14, 2024 - August 12, 2024 (UTC)

Unique IPs Observed

https://viz.greynoise.io/tags/apache-ofbiz-cve-2024-32113-path-traversal-attempt?days=30

Last 30 days



Ruijie RG-UAC CVE-2024-4813 RCE Attempt

WE NEED

TO TALK

ABOUT

KEV

STORM WATCH

It Has Been

1

Days Since The
Last KEV Release

https://kev.hrbrmstr.app

CVE-2018-0824: Microsoft COM for Windows Deserialization of Untrusted Data

CVE-2024-32113: Apache OFBiz Path Traversal Vulnerability 🏷️

CVE-2024-36971: Android Kernel Remote Code Execution