STORM WATCH

CYBERSECURITY NEWS

# Dateline: 2024-07-16

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

STORM WATCH

CYBERSECURITY NEWS

# CYBERSIDE CHAT

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-193a

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory

CYBERSECURITY ADVISORY

# CISA Red Team's Operations Against a Federal Civilian Executive Branch Organization Highlights the Necessity of Defense-in-Depth

**Release Date:** July 11, 2024

**Alert Code:** AA24-193A

In early 2023, the Cybersecurity and Infrastructure Security Agency (CISA) conducted a SILENTSHIELD red team assessment against a Federal Civilian Executive Branch (FCEB) organization. During SILENTSHIELD assessments, the red team first performs a no-notice, long-term simulation of nation-state cyber operations. The team mimics the techniques, tradecraft, and behaviors of sophisticated threat actors and measures the potential dwell time actors have on a network, providing a realistic assessment of the organization's security posture. Then, the team works directly with the organization's network defenders, system administrators, and other technical staff to address strengths and weaknesses found during the assessment. The team's goal is to assist the organization with refining their detection, response, and hunt capabilities—particularly hunting unknown threats.

# Key Findings

- Red team gained initial access by exploiting an unpatched vulnerability and through phishing
- Discovered unsecured admin credentials, allowing full domain compromise
- Pivoted to external partner organizations due to trust relationships
- Remained undetected throughout first phase of assessment
- Organization only understood full extent of compromise by analyzing all data sources

# Lessons Learned

- Insufficient controls to prevent and detect malicious activity
- Ineffective collection, retention and analysis of logs
- Bureaucratic processes and decentralized teams hindered network defenders
- "Known-bad" detection approach hampered identifying alternate TTPs
- Over-reliance on specific IOCs rather than behavior-based detection

# Key Recommendations

- Apply defense-in-depth principles with multiple layers of security
- Implement robust network segmentation to impede lateral movement
- Establish baselines for network traffic, application execution, and authentication
- Use an "allowlist" approach rather than denying known-bad IOCs
- Ensure detection is primarily behavior-based rather than IOC-centric
- Improve log collection, retention and analysis capabilities

STORM WATCH

CYBERSECURITY NEWS

# CYBER SPOTLIGHT


https://vimeo.com/314294745

# Have you ever sent a postcard you didn't have to mail?

**YOU WILL**℠

In the near future your correspondence, from postcards to memos, will be immediate.

Transmitted instantly, from the screen of your personal communicator to someone else's. Or to their E-mail or fax. No paper. No pen. No postage.

Notes from thin air.

The company that will bring it to you is AT&T.

AT&T

# Have you ever seen a global multinational mishandle the Call Data Records of millions of hapless customers?

**YOU WILL**℠

One day, irresponsible data analysts who want "Snowflake" on their resumes, will needlessly move CDRs to "the cloud", and Snowflake's equally irresponsible governance policies will fail to enforce multi-factor authentication, allowing attackers to conduct one of the biggest supply chain breaches in history.



AT&T

https://about.att.com/story/2024/addressing-illegal-download.html

AT&T announced a massive data breach affecting "nearly all" of its wireless customers. The breach occurred between April 14 and April 25, 2024, when hackers illegally accessed and exfiltrated customer data from AT&T's workspace on a third-party cloud platform, which was later confirmed to be Snowflake.

- Phone records of calls and text messages from May 1, 2022, to October 31, 2022, and some records from January 2, 2023
- Phone numbers of AT&T cellular and landline customers, as well as customers of other carriers who interacted with AT&T numbers
- Call and text metadata, including call durations and frequency of interactions
- Cell site identification numbers for some records, potentially revealing approximate locations of calls and texts

The breach is part of a larger cybersecurity incident involving Snowflake, a cloud data platform used by many companies for data analysis. This attack has affected multiple Snowflake customers, including Ticketmaster, Santander Bank, Neiman Marcus, and LendingTree.

Attackers exploited a lack of multi-factor authentication in some Snowflake customer accounts, using stolen credentials to gain unauthorized access. The malware infections in Snowflake's systems reportedly date back to 2020, with some stolen credentials remaining valid for years.

The cybercriminal group responsible for the attack has been identified as UNC5537 by Mandiant, a cybersecurity firm. This financially motivated group is believed to have members in North America and Turkey.

In a surprising twist, AT&T reportedly paid a hacker affiliated with the ShinyHunters group over $300,000 in Bitcoin to delete the stolen data and provide video evidence of its deletion. However, there are concerns that other entities may still have copies of the data.

The breach has affected a vast number of AT&T's 242 million U.S. wireless customers and 128 million connected devices. AT&T is notifying affected customers and has taken steps to close off the illegal access point.

*"AT&T received a national security exception from DOJ under the SEC reporting requirements. First such exception I'm aware of."*

— Christopher Krebs, former director of CISA

STORM WATCH

CYBERSECURITY NEWS

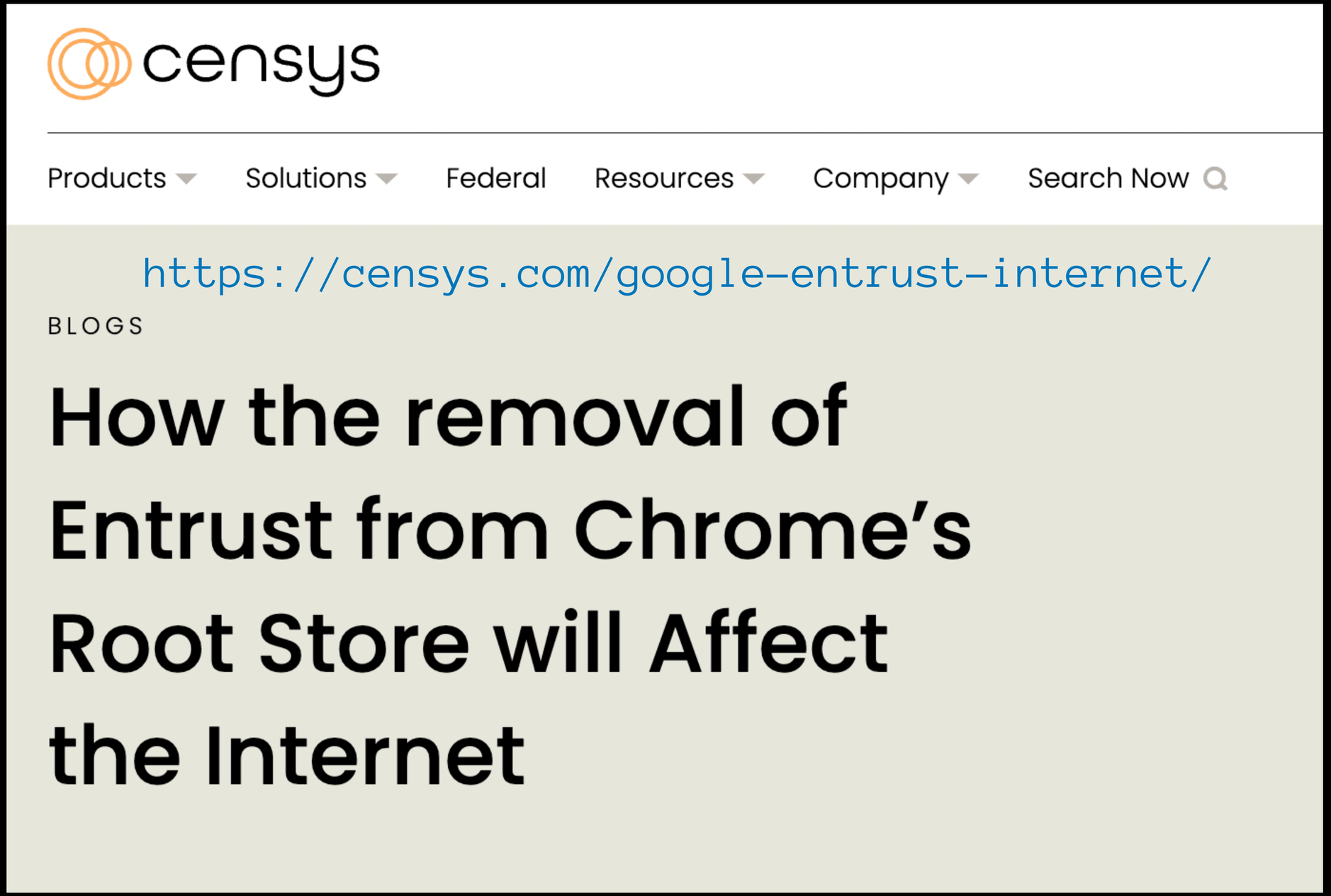
# SHAMELESS SELF-PROMOTION

VULNERABILITIES

# Perma-Vuln: D-Link DIR-859, CVE-2024-0769

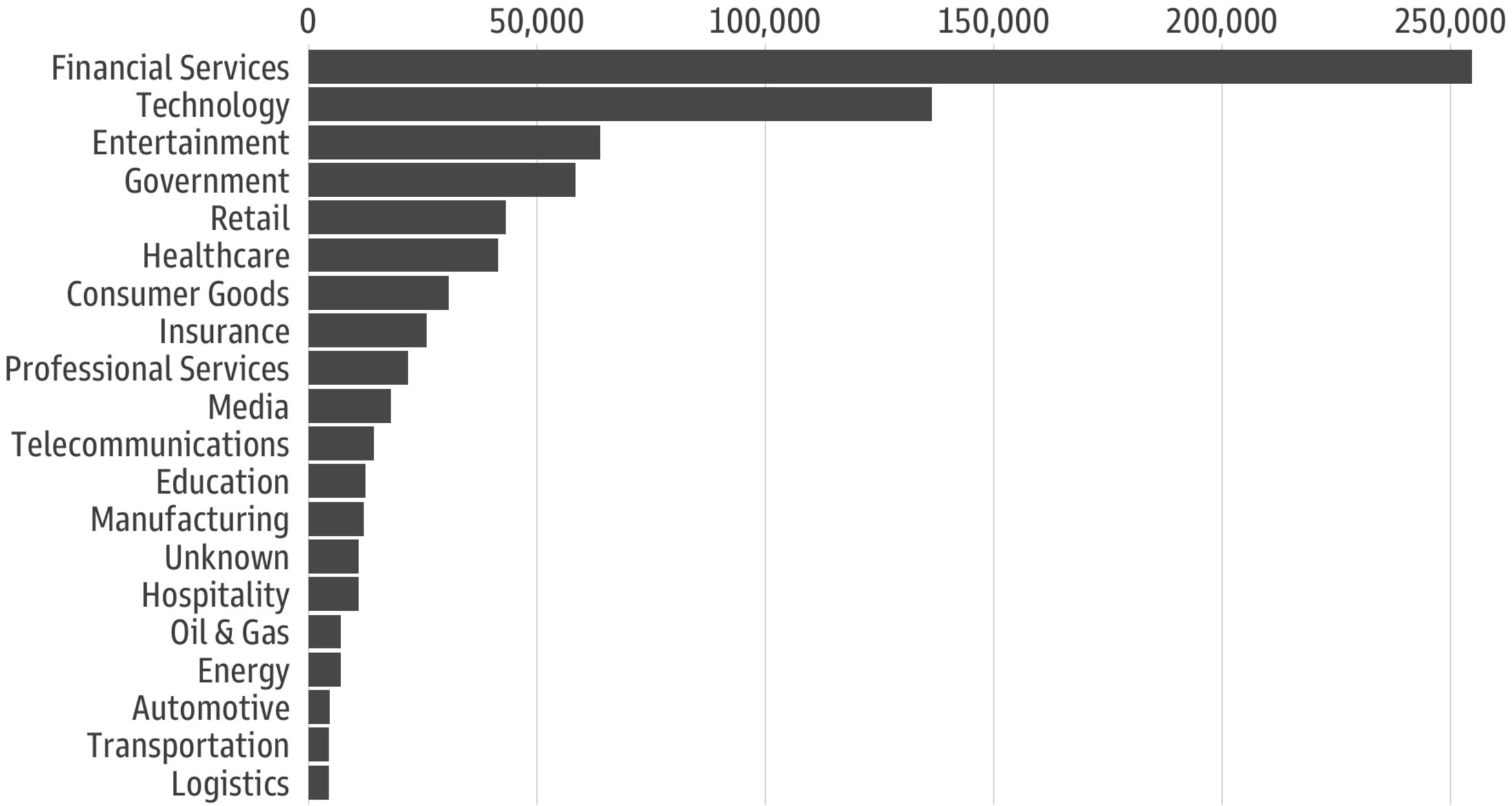
The GreyNoise Labs Team | June 27, 2024


https://www.greynoise.io/blog/perma-vuln-d-link-dir-859-cve-2024-0769

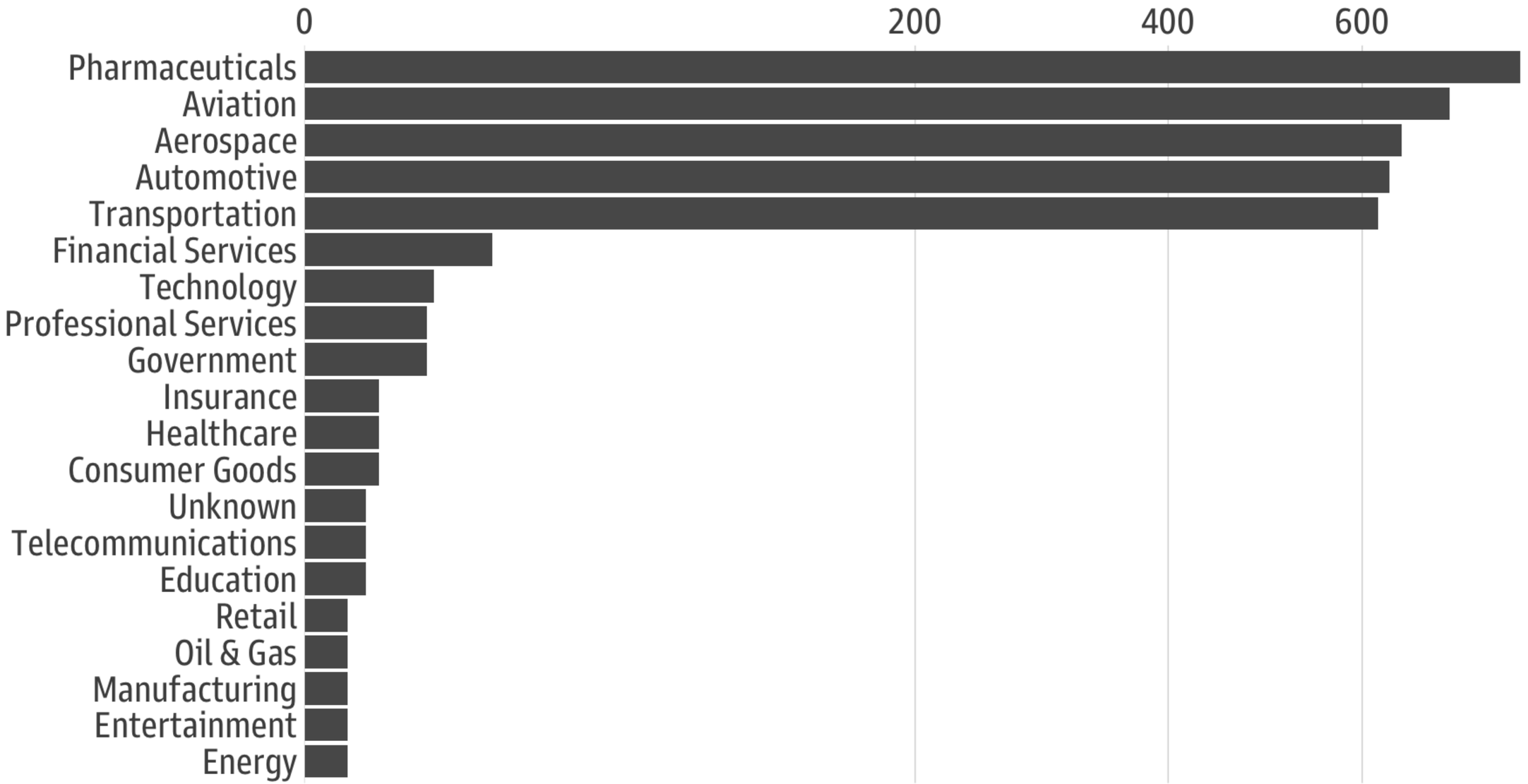



https://security.googleblog.com/2024/06/sustaining-digital-certificate-security.html

## Industry Host Count

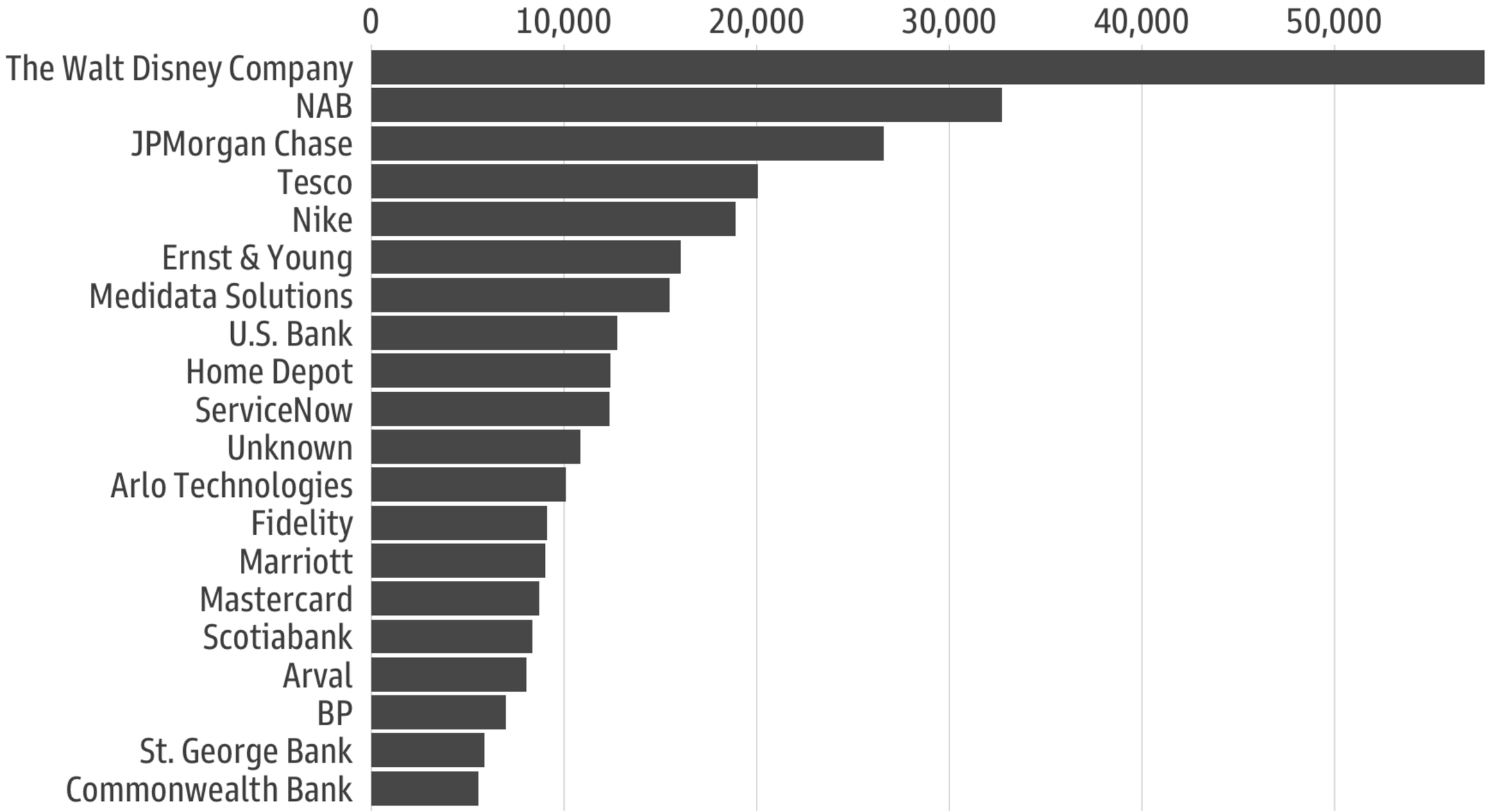


## Industry Leaf Count

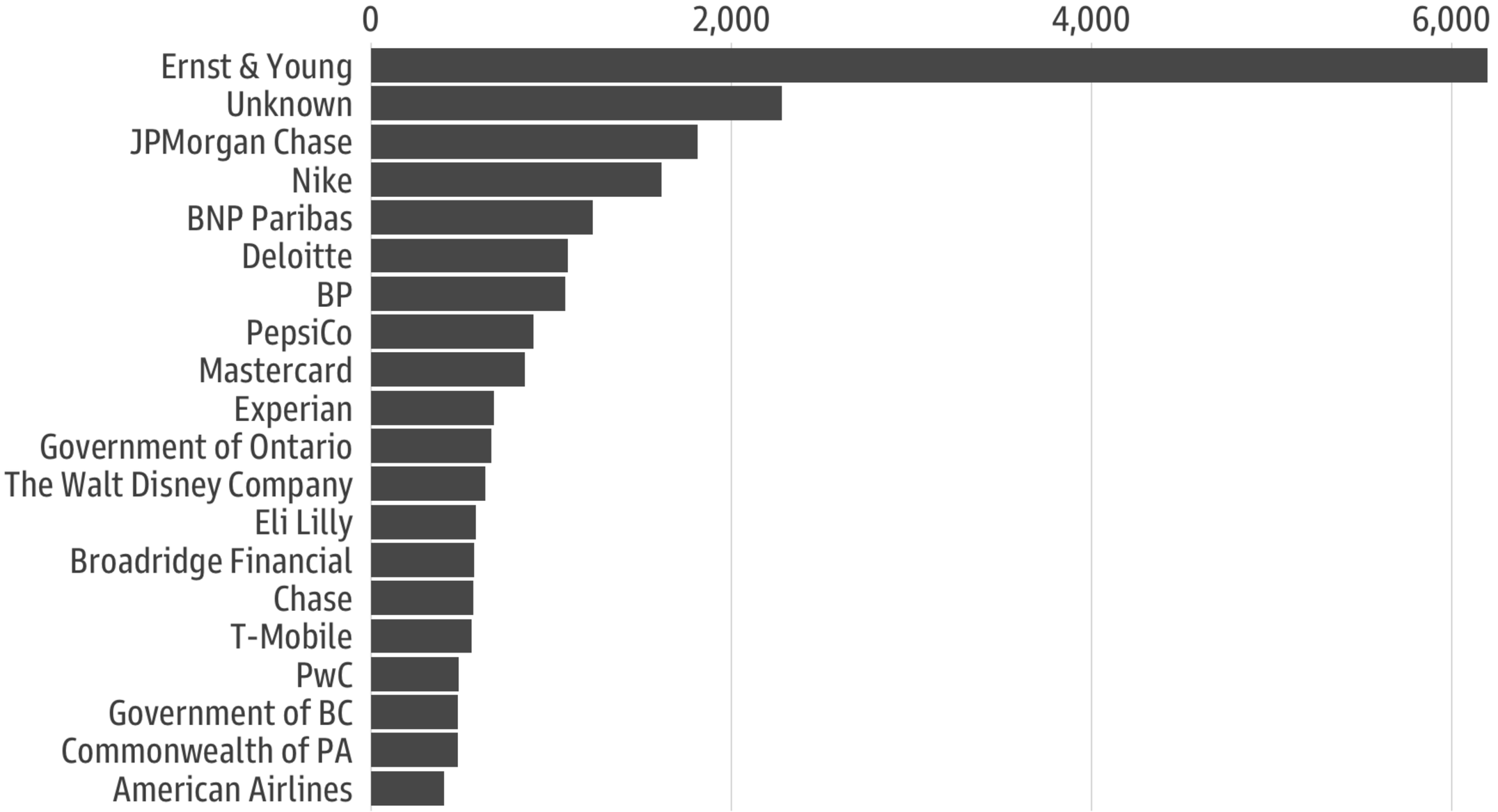



NOTE sqrt scale

## Organization Host Count



## Organization Leaf Count



STORM WATCH

CYBERSECURITY NEWS

# TAG ROUND-UP

D-Link DIR-859 Information Disclosure Attempt

D-Link Devices HNAP SOAPAction Header RCE Attempt

LeagueManager SQL Injection Attempt

MoveIT Transfer CVE-2024-5806 Logfile Manipulation Attempt

PHP DebugBar Information Disclosure Attempt

Palo Alto Networks Login Scanner

Selenium RemoteWebDriver Scanner

Symfony Fragment Scanner

VMware Server CVE-2009-3733 Path Traversal Attempt

WordPress Fusion Builder SSRF CVE-2022-1386 Attempt

WE NEED

TO TALK

ABOUT

KEV

STORM WATCH

It Has Been

# 1

Days Since The
Last KEV Release

https://kev.hrbrmstr.app

CVE-2020-13965: Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability

CVE-2022-2586: Linux Kernel Use-After-Free Vulnerability

CVE-2022-24816: OSGeo GeoServer JAI-EXT Code Injection Vulnerability

CVE-2024-20399: Cisco NX-OS Command Injection Vulnerability

CVE-2024-23692: Rejetto HTTP File Server Improper Neutralization of Special Elements Used in a Template Engine Vulnerability

CVE-2024-38080: Microsoft Windows Hyper-V Privilege Escalation Vulnerability

CVE-2024-38112: Microsoft Windows MSHTML Platform Spoofing Vulnerability

CVE-2024-36401: OSGeo GeoServer GeoTools Eval Injection Vulnerability