The Persistent Threat of Salt Typhoon: Tracking Exposures of Potentially Targeted Devices

censys.com/blog/the-persistent-threat-of-salt-typhoon-tracking-exposures-of-potentially-targeted-devices

Executive Summary

- **Salt Typhoon** (also known as FamousSparrow/GhostEmperor/RedMike/UNC2286) is a Chinese state-sponsored threat actor that has compromised major telecommunications providers worldwide
- Although confirmed IOCs for Salt Typhoon remain sparse, public reporting suggests that their campaigns against telecommunications providers target known vulnerabilities in publicly available network device interfaces to gain initial entry
- We track global exposures of internet-facing network devices associated–either loosely or directly–with Salt Typhoon activity over the past six months, including: Sophos Firewalls, Cisco IOS XE WebUIs, Ivanti Connect Secure, and Fortinet FortiClient EMS systems. When version data was available, we also measured how many devices were running versions known to be vulnerable to the CVEs discussed.
- It's important to note that in this campaign, **even fully patched device exposures can potentially pose a risk**, as Salt Typhoon and similar actors often bypass exploitation entirely by using stolen credentials. Understanding how exposure has evolved over time can help us assess both the evolving scale of the threat from this campaign and how organizations may be responding at large
- While definitive attribution to Salt Typhoon remains vague, these network device vulnerabilities represent critical security priorities in that they often provide direct access to internal networks and sensitive resources
- A six-month trend analysis reveals:
    - Overall **combined exposure** of tracked network devices has **decreased by 25%** since October 2024.
    - The **largest reduction** came from **Sophos Firewall web interfaces**, which saw a **35% drop** in exposures (over 70,000 instances)
    - **Cisco IOS XE** was the **only platform to show a net increase**, albeit minimal, with exposures **rising by approximately 7%** (over 3,000 instances)
    - Ivanti Connect Secure and FortiClient EMS exposures showed **minimal net change**, but trended **slightly downward**, with decreases by 13% and 3% respectively
- Geographically, the majority of current exposures remain concentrated in the **United States,** except for Sophos XG Firewall exposures which are concentrated in **Germany**

- The persistence of relatively large numbers of these devices on the internet raises key questions about why these systems are still online and what large drops in exposure may actually reflect: successful remediation, routine device reconfigurations, or something else.

Background

State-sponsored threat actors have increasingly targeted network infrastructure– routers, VPNs, and other edge devices essential to securing the perimeter. Among them, **Salt Typhoon** (also known as Earth Estries, FamousSparrow, GhostEmperor, RedMike, and UNC2286), a threat group linked to the PRC, has gained attention for its systematic exploitation of known network device vulnerabilities against telecommunications providers and public sector environments.

This has included major incidents such as breaches of U.S. telecommunications providers, as reported by CISA and various media sources. In these campaigns, the group often gains access by exploiting unpatched network devices, like Cisco routers, to gain persistent access to sensitive infrastructure and conduct follow-on exploits. They are known for leveraging stealthy techniques such as disabling logs, routing through compromised infrastructure, and avoiding traditional malware payloads entirely–relying instead on living-off-the-land techniques and direct manipulation of device settings These tactics can make detection difficult for organizations that rely on endpoint security monitoring.

This blog analyzes a set of known network device vulnerabilities that have been linked–though often tentatively–to Salt Typhoon in public reporting, and examines the global exposure of potentially affected devices. We'll look at which devices are most affected, how their exposure has shifted over time, and why addressing these vulnerabilities is critical to defending against future campaigns. While direct evidence of exploitation varies and confirmed IoCs remain rare, these vulnerabilities are nevertheless worth monitoring given their susceptibility to threats.

It's also worth noting that while CVEs are useful markers for tracking risk, threat actors often bypass the need to exploit altogether and simply log in. As Talos observed, in most incidents involving Cisco devices, access was gained through stolen credentials rather than exploited vulnerabilities. As such, even fully patched devices can be at risk. Monitoring all exposed network device interfaces on your systems remains critical.

Understanding the Known Vulnerabilities Linked to Salt Typhoon

We analyzed CVEs in four distinct network device products that have appeared frequently in connection with Salt Typhoon across multiple intelligence sources, although this isn't an exhaustive list. Attribution remains difficult due to Salt Typhoon's use of sophisticated

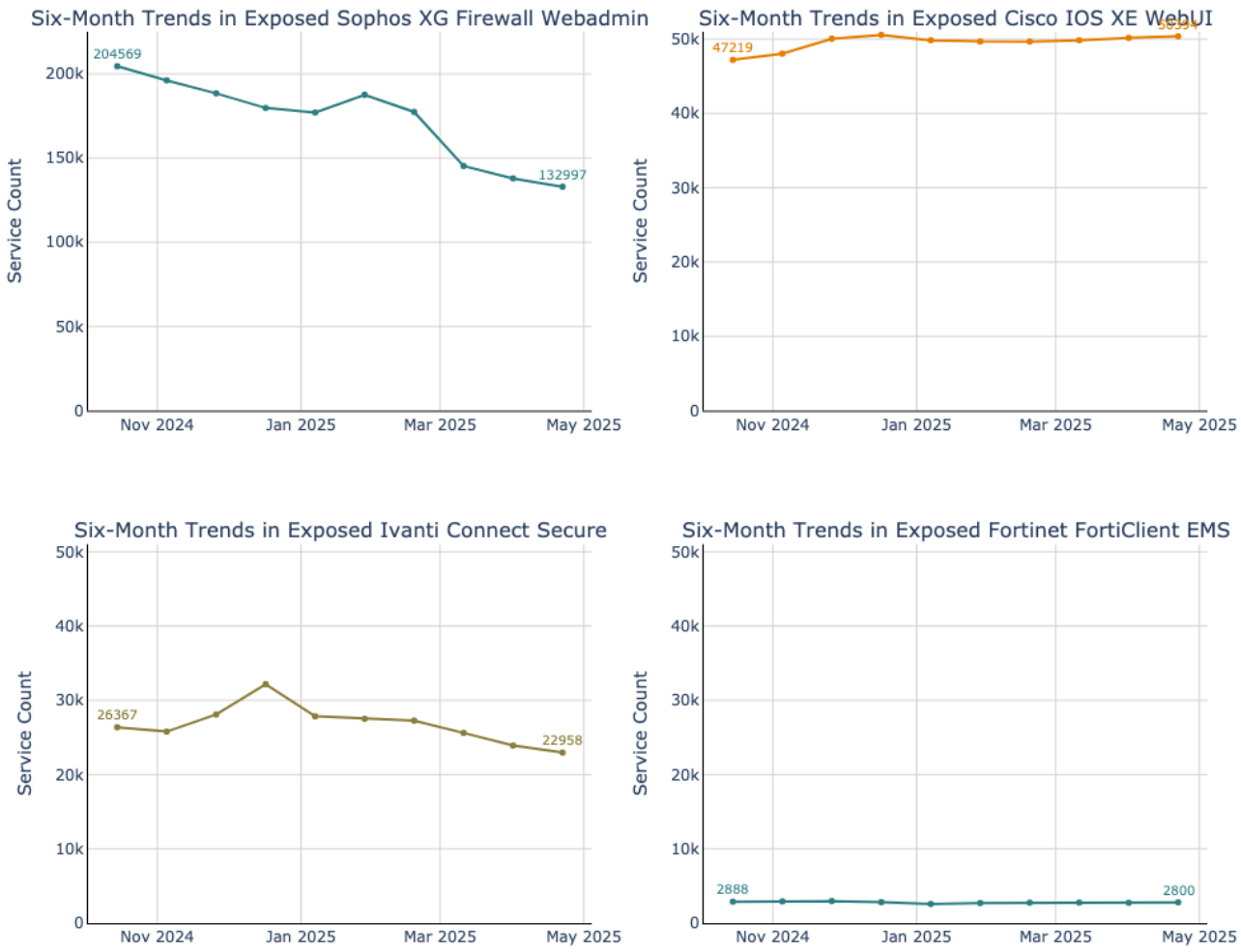
evasion techniques, with much **activity being associated based on inferences rather than direct first-party evidence**.

However, these vulnerabilities deserve attention regardless of their specific attribution status, since **network devices continue to be frequently targeted by multiple threat actor groups**, and **all have patches available**.

CVE	Description	CVSS Score	Date of Disclosure	Patch Information
CVE-2022-3236	Sophos Firewall RCE	9.8	9/23/2022	Source
CVE-2023-20198	Cisco IOS XE Web UI Privilege Escalation	10.0	10/16/2023	Source
CVE-2023-20273	Cisco IOS XE Web UI Command Injection	7.2	10/16/2023	Source
CVE-2023-46805	Ivanti Connect Secure Authentication Bypass	8.2	01/10/2024	Source
CVE-2024-21887	Ivanti Connect Secure Command Injection	9.1	01/10/2024	Source
CVE-2023-48788	Fortinet FortiClient EMS SQL Injection	9.8	02/22/2024	Source

Comparing Six-Month Exposure Trends Across All Affected Devices

For each device, we examine exposure trends over the **past six months** from October 2024 to April 2025 to assess how the attack surface landscape has evolved in the aftermath of public disclosure of Salt Typhoon's recent campaign against telecommunications companies and the federal government.



Note that Sophos XG Firewall data uses a different vertical scale to properly visualize its significantly higher exposure count compared to the other studied devices.

Current Levels of Exposure:

Device	Exposures as of April 22, 2025
Sophos XG Firewall Webadmin	132,997
Cisco IOS XE WebUI	50,394
Ivanti Connect Secure	22,958
Fortinet FortiClient EMS	2,800

These trends reveal a few key insights:

- The **combined exposure** of network devices tracked in this analysis has **decreased by 25%** since October 2024. This could be owing to any number of reasons, a few of which might be a shift in defensive posture or increased awareness of these risks.
- This reduction was driven primarily by **Sophos Firewall web interfaces**, which saw a **35% drop (over 70,000 fewer exposed instances)**, marking the most significant decline across all platforms.
- **Cisco IOS XE WebUI** exposures were the exception, **increasing by approximately 7%** (over **3,000 additional instances**), making it the only platform to show a net increase in publicly accessible interfaces.
- **Ivanti Connect Secure** and **FortiClient EMS** exposures showed **minor decreases**, down **13%** and **3%** respectively, indicating more consistent—but still exposed—attack surfaces.
- The current **absolute scale of exposure as of April 2025** varies widely across different devices– **Sophos Firewall web interfaces** account for around **133,000** exposed instances compared to about **3,000** for **FortiClient EMS**– suggesting a larger potential attack surface for Cisco-related vulnerabilities
- **Cisco IOS XE's upward trend in exposure**, despite increased attention to its vulnerabilities and active exploitation by threat actors, raises important questions about why these interfaces remain publicly accessible online–given that they are primarily intended for device management and configuration, **not for public-facing services**. Cisco has recommended mitigating CVE-2023-20198 by **limiting access to the HTTP Server to trusted networks** to reduce exposure to these vulnerabilities.

In the following section, we examine each potentially targeted vulnerability, assessing its reported connection to Salt Typhoon and analyzing both current and historical exposure levels. While these devices are **all publicly accessible, not all are necessarily vulnerable**—yet their presence alone expands the attack surface and renders organizations more at risk of opportunistic scanning by threat actors. Even patched systems can be at risk if valid credentials are compromised, making consistent exposure monitoring essential. This is especially critical for sectors like telecommunications and government, which remain key targets for Salt Typhoon.

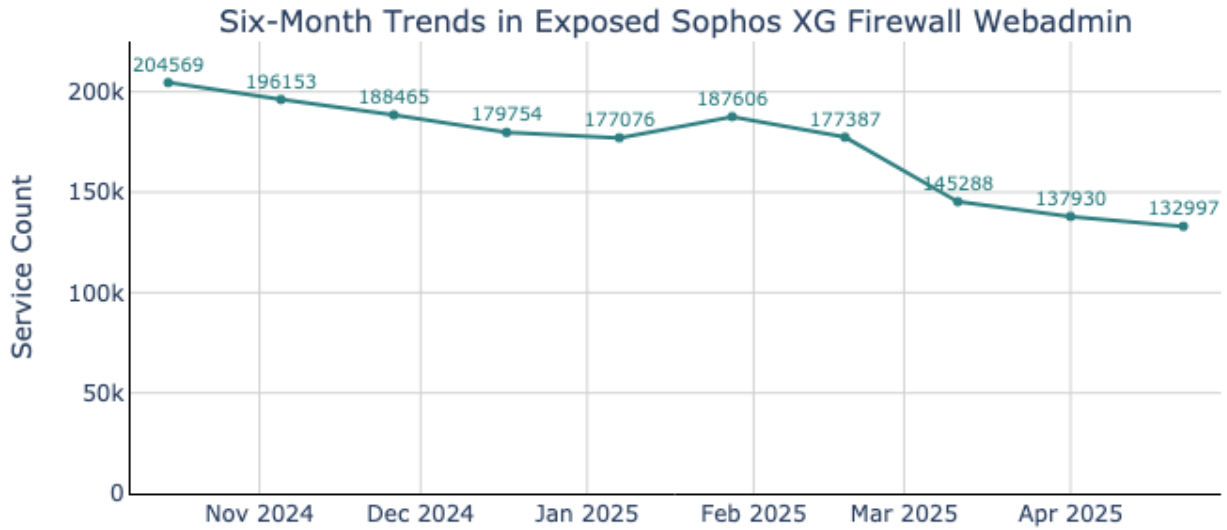
Sophos Firewall RCE [CVE-2022-3236]

- **Vulnerability Type: Code Injection / RCE**
- **Affected Products: Sophos Firewall v19.0 MR1 (19.0.1) and older**
- **CVSS Score: 9.8**
- **Technical Impact: Exploitable via the User Portal or Webadmin, allowing remote code execution without authentication.**

This critical vulnerability enabled unauthenticated RCE through the web interfaces of certain versions of Sophos Firewalls. Trend Micro's research on Salt Typhoon (dubbed "Earth Estries") noted a potential connection to this vulnerability, stating they "currently only have

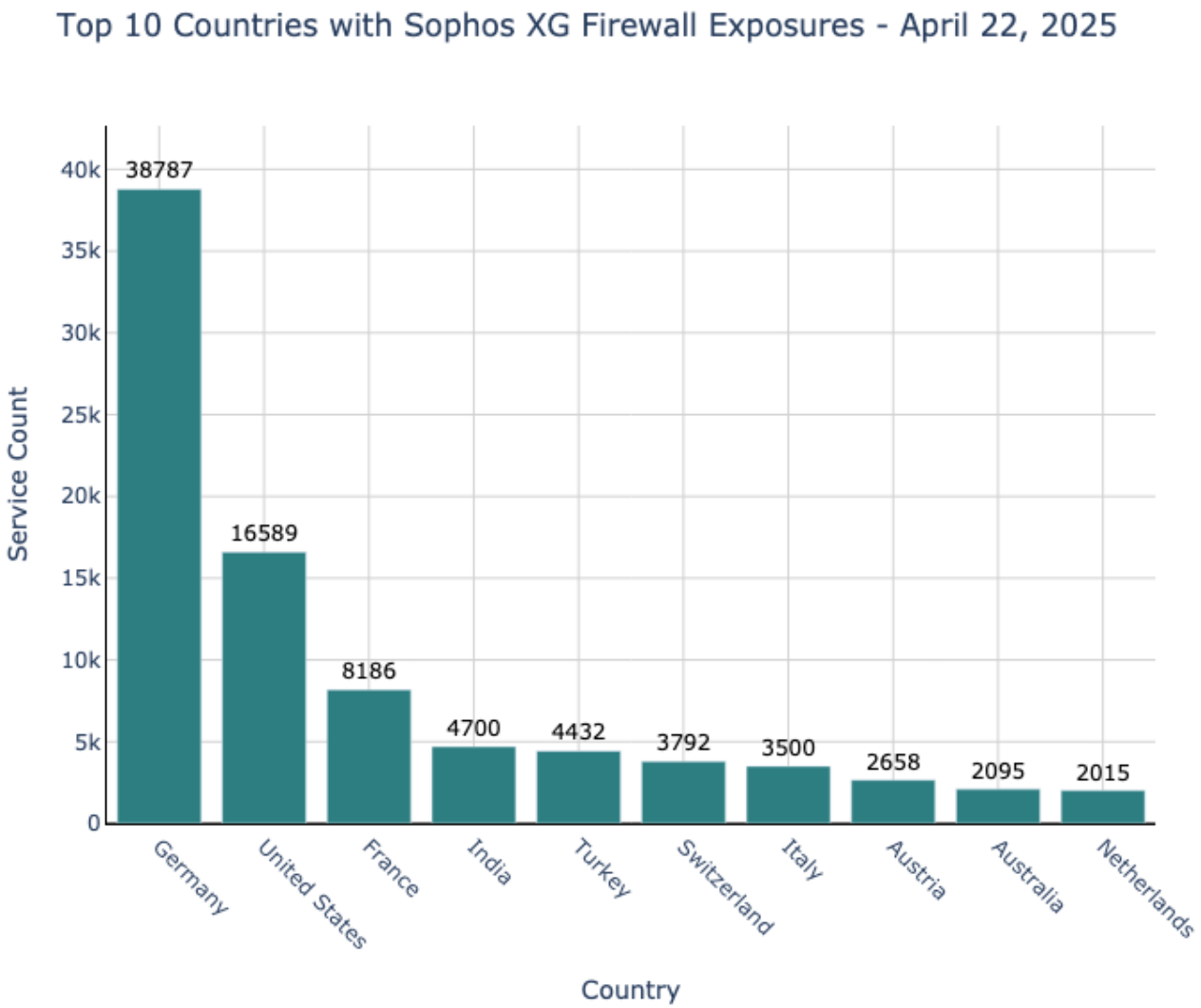
low confidence that Earth Estries has previously deployed the MASOL RAT through CVE-2022-3236" and that they cannot rule out the possibility that MASOL RAT is a shared tool among limited Chinese APT threat groups."

Exposure Snapshot: As of April 2025, Censys observed **132,997 exposed Sophos XG Firewall** web interfaces, of which **9,462** were explicitly advertising a version that may potentially be vulnerable to CVE-2022-3236. Comparatively, there were **204,569** overall exposed devices in October 2024. That's a marked reduction by nearly 35% of exposures, and the most dramatic decrease we saw across all the network device products we tracked.



This graph shows a gradual but steady decline in exposed Sophos Firewall XG web interfaces over the past six months, with a total drop of 71,572 devices since October 2024. Notably, January saw a brief and unusual spike—exposures increased by over 10,000 devices, followed quickly by a sharp drop. This type of rapid change is rare for firewall products, which typically have stable configurations, and this pattern doesn't align with any known Sophos vulnerability disclosures or security advisories. One possible explanation is that the spike reflects a wave of honeypot deployments or new service configurations prompted by increased threat intelligence and vendor alerts related to Salt Typhoon activity at the start of the new year.

We then examined where most of the current exposures are hosted geographically, with exposure data from April 22, 2025.



Interestingly, Germany appears to have a dramatically higher concentration of Sophos exposures with 38,787 instances, more than double the 16,589 found in the United States. This is particularly striking given that Germany hosts far fewer internet-facing services than the U.S. overall.

Cisco IOS XE Web UI Privilege Escalation [CVE-2023-20198] and Command Injection [CVE-2023-20273]

CVE-2023-20198:

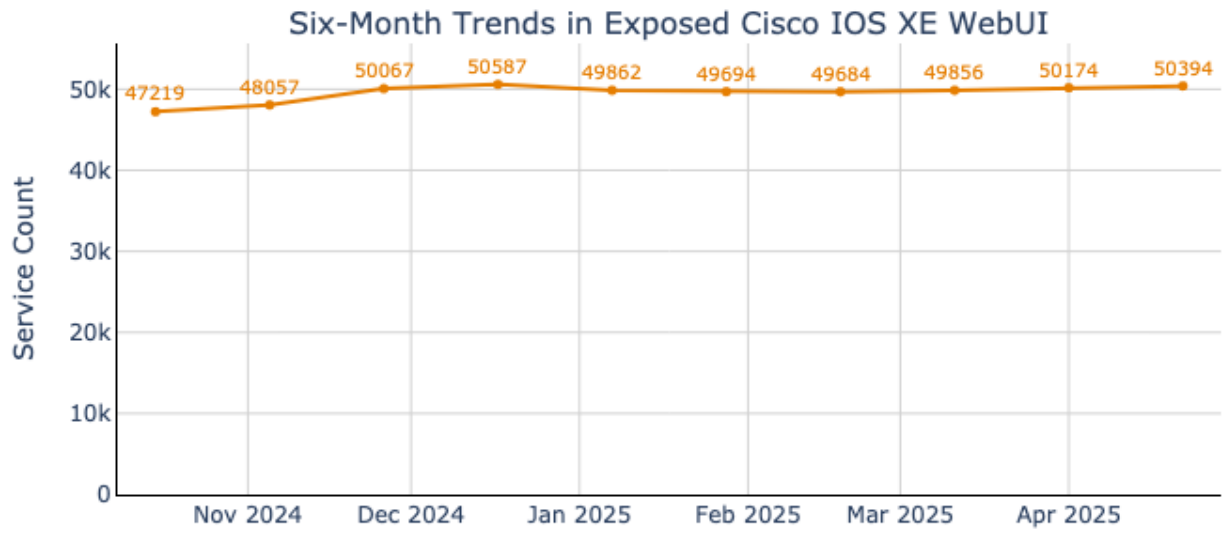
- **Vulnerability Type:** Privilege Escalation Vulnerability
- **Affected Products:** Web feature in Cisco IOS XE software
- **CVSS Score:** 10.0
- **Technical Impact:** This vulnerability allows unauthenticated attackers to create a privileged level 15 user account through the Web UI. Combined with CVE-2023-20273, it enables full control over vulnerable Cisco IOS XE devices.

CVE-2023-20273:

- **Vulnerability Type:** Command Injection Vulnerability
- **Affected Products:** Web feature in Cisco IOS XE software
- **CVSS Score:** 7.2
- **Technical Impact:** This vulnerability allows an authenticated attacker to perform command injection with root privileges. Combined with CVE-2023-20198, it enables full control over vulnerable Cisco IOS XE devices.

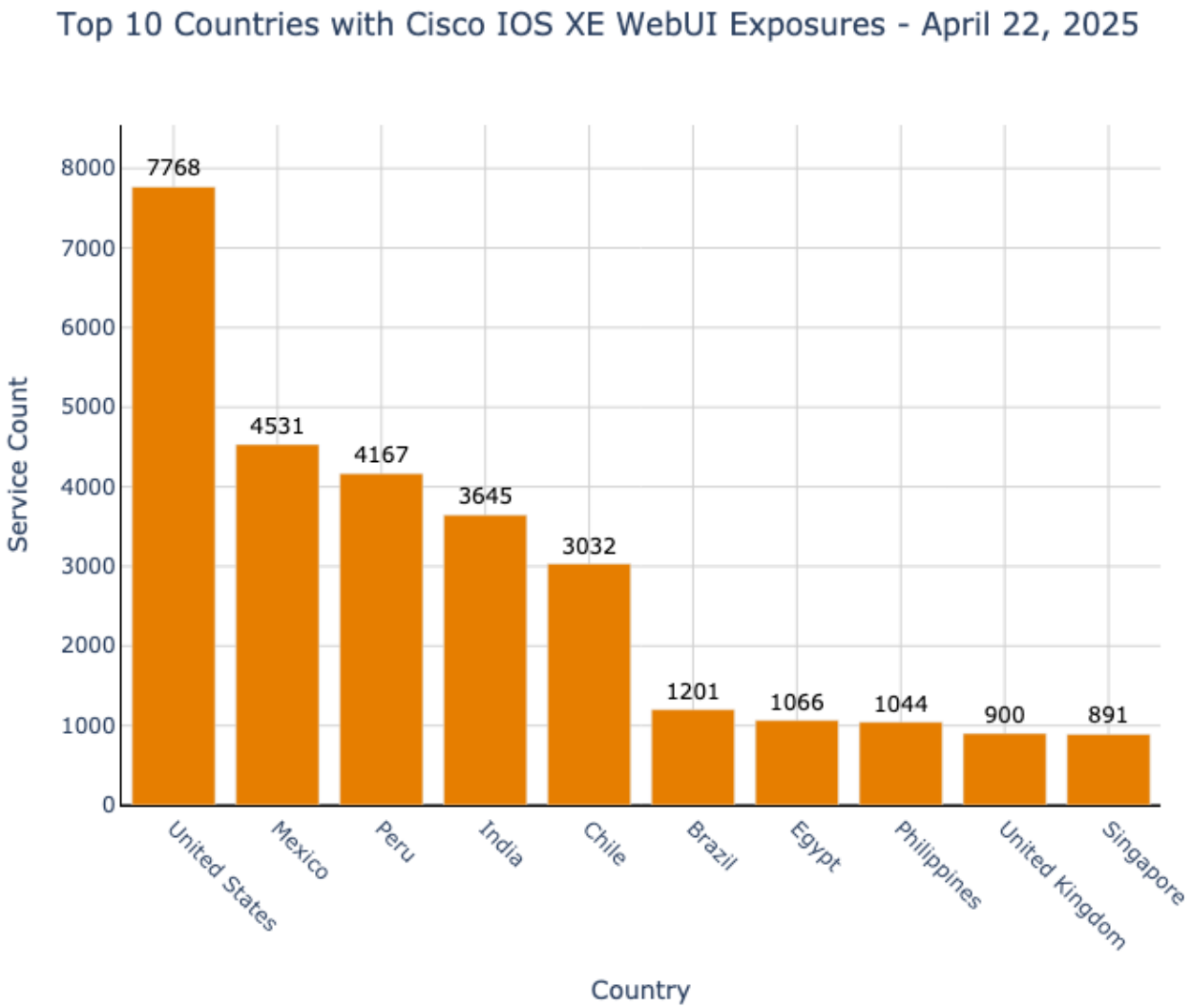
CVE-2023-20198 is one of the more severe network device vulnerabilities of the past few years, allowing unauthenticated remote attackers to create admin accounts and compromise affected devices. RecordedFuture reported observing Salt Typhoon exploiting this vulnerability in a chain along with CVE-2023-20273 against devices associated with telecommunications providers in particular, noting: “RedMike has attempted to exploit over 1,000 internet-facing Cisco network devices worldwide, primarily those associated with telecommunications providers, using a combination of two privilege escalation vulnerabilities: CVE-2023-20198 and CVE-2023-20273.” They have then been observed to change device configurations and establish GRE tunnels for persistent access.

Exposure Snapshot: As of April 2025, Censys observed **50,394** exposed devices that may potentially be affected by CVE-2023-20198 and CVE-2023-20273 compared to **47,219** exposed devices in October 2024. This snapshot reflects the total number of *exposed*, but not necessarily vulnerable devices, *as we do not have specific version information available.*



Interestingly, the number of exposed devices increased moderately from October to December 2024, climbing by 4,000 devices, before plateauing at around 50,000 instances. The minor monthly fluctuations in device counts likely represent routine infrastructure

changes rather than coordinated patching or segmentation efforts. This relatively high level of exposure is concerning given the widespread warnings of exploitation of this threat.



The United States currently hosts the most exposed Cisco IOS XE Web UIs as of April 22, 2025 with 7,778 instances. Overall these exposures are mostly concentrated in the Americas, with five countries (U.S., Mexico, Peru, Brazil, and Chile) accounting for 60% of the top exposures worldwide.

Ivanti Connect Secure Authentication Bypass [CVE-2023-46805] and Command Injection [CVE-2024-21887]

CVE-2023-46805:

- **Vulnerability Type:** Authentication Bypass
- **Affected Products:** Ivanti Connect Secure and Policy Secure
- **CVSS Score:** 8.2

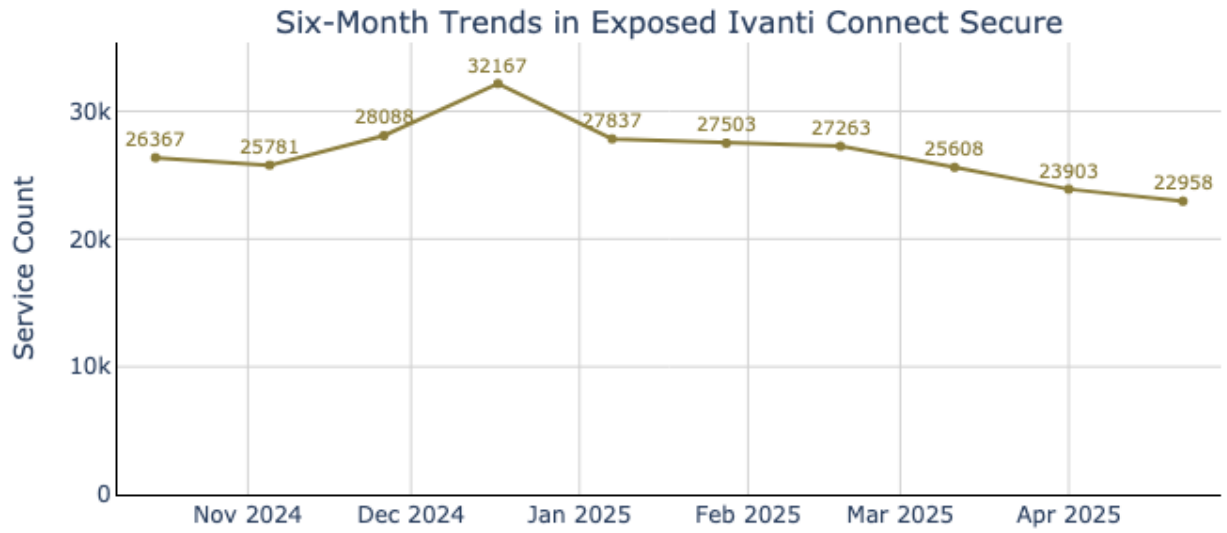
- **Technical Impact:** Allows unauthenticated attackers to bypass authentication controls. Commonly exploited in conjunction with CVE-2024-21887, enabling remote command execution and full system compromise.

CVE-2024-21887:

- **Vulnerability Type:** Command Injection
- **Affected Products:** Ivanti Connect Secure and Policy Secure
- **CVSS Score:** 9.1
- **Technical Impact:** Allows remote, unauthenticated attackers to execute commands with elevated privileges, potentially leading to full system compromise

Trend Micro's report on Earth Estries/Salt Typhoon states that the group actively exploits Ivanti Connect Secure VPN flaws to establish initial access to targeted networks. Their report notes a connection between specific command and control infrastructure and IoCs of the Ivanti exploits: "The frpc C&C 165.154.227[.]192 could be linked to an SSL certificate (SHA256: 2b5e7b17fc6e684ff026df3241af4a651fc2b55ca62f8f1f7e34ac8303db9a31) previously used by ShadowPad, which is another shared tool among several Chinese APT groups. In addition, the C&C IP address was also mentioned in a Fortinet report and indicators of compromise related to the Ivanti exploit."

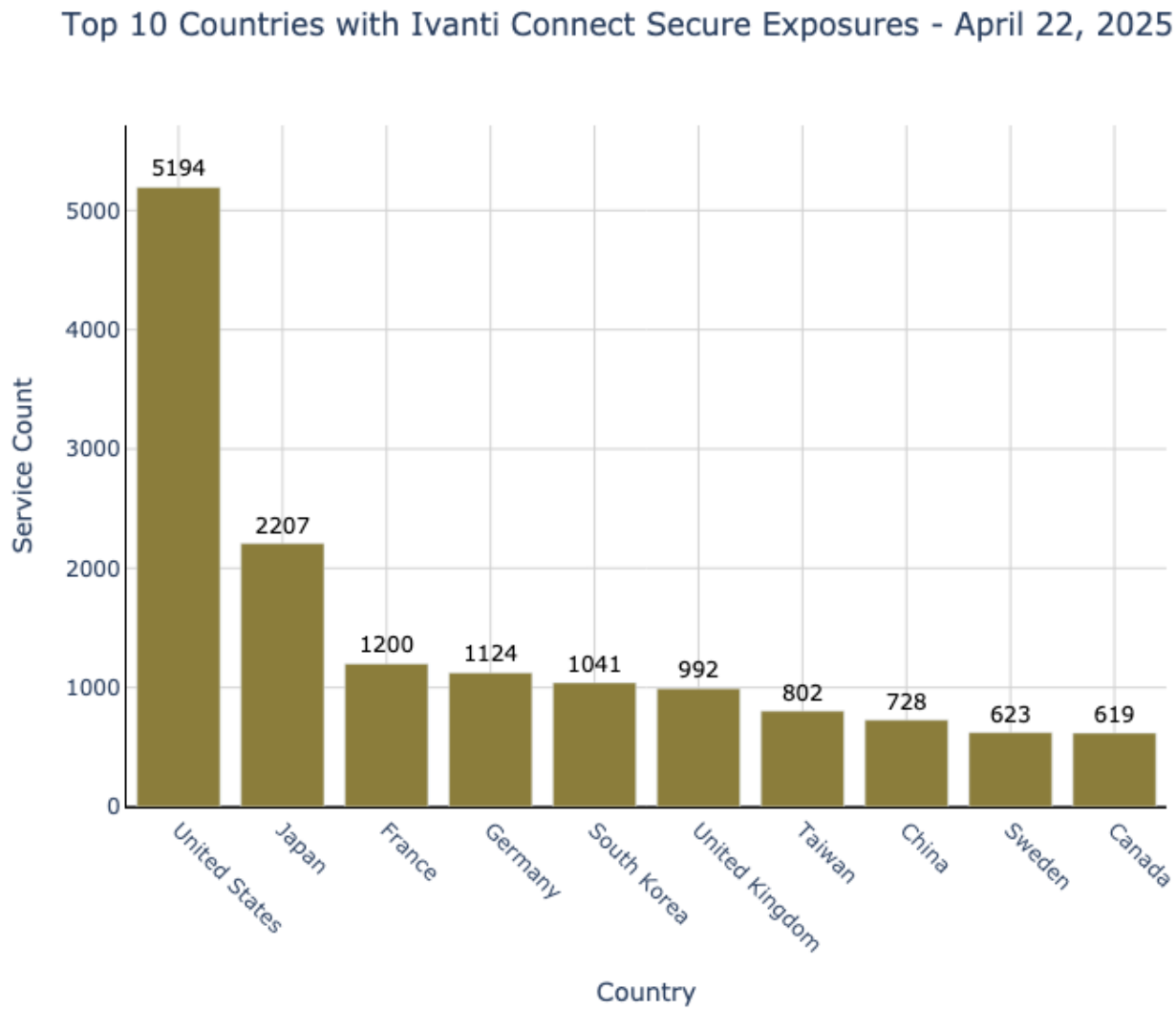
Exposure Snapshot: As of April 2025, Censys observed **22,958** exposed devices that may potentially be vulnerable to CVE-2023-46805, with **5,290** advertising a software version that is vulnerable to the exploit. By contrast, we saw **26,367** exposed devices in October 2024.



There was a noticeable spike of 3,000 additional exposed Ivanti Connect Secure instances online in mid-December 2024–the timing of which interestingly coincided with Ivanti's disclosure of six additional vulnerabilities in their Connect Secure and Policy Secure products. It's possible that a portion of these new hosts were honeypots deployed by

organizations in response to the advisory–although odd that the increase was gradual, and started back in early November. Since then, exposure has steadily declined, although at a slow pace.

Additionally, on April 23 GreyNoise "observed a 9X spike in suspicious scanning activity targeting Ivanti Connect Secure (ICS) or Ivanti Pulse Secure (IPS) VPN systems." They noted seeing 230 malicious IPs scanning ICS/IPS endpoints and suggested this activity may be related to "coordinated reconnaissance and possible preparation for future exploitation."



As of April 22, 2025, the United States has the highest concentration of Ivanti Connect Secure exposures, with 5,194 instances–more than double Japan's 2,207 exposures in second place and over four times the exposure count of any other country in the top ten. Other exposures are spread broadly across Asia, Europe, and North America.

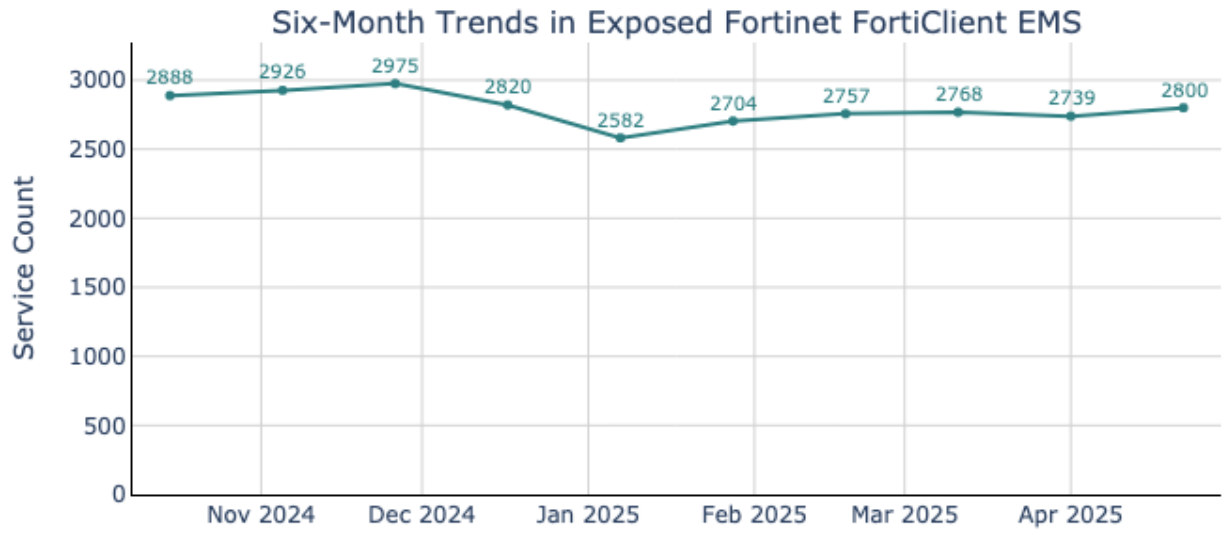
Fortinet FortiClient EMS SQL Injection [CVE-2023-48788]

- **Vulnerability Type: SQL Injection**
- **Affected Products: FortiClient Enterprise Management Server (EMS)**

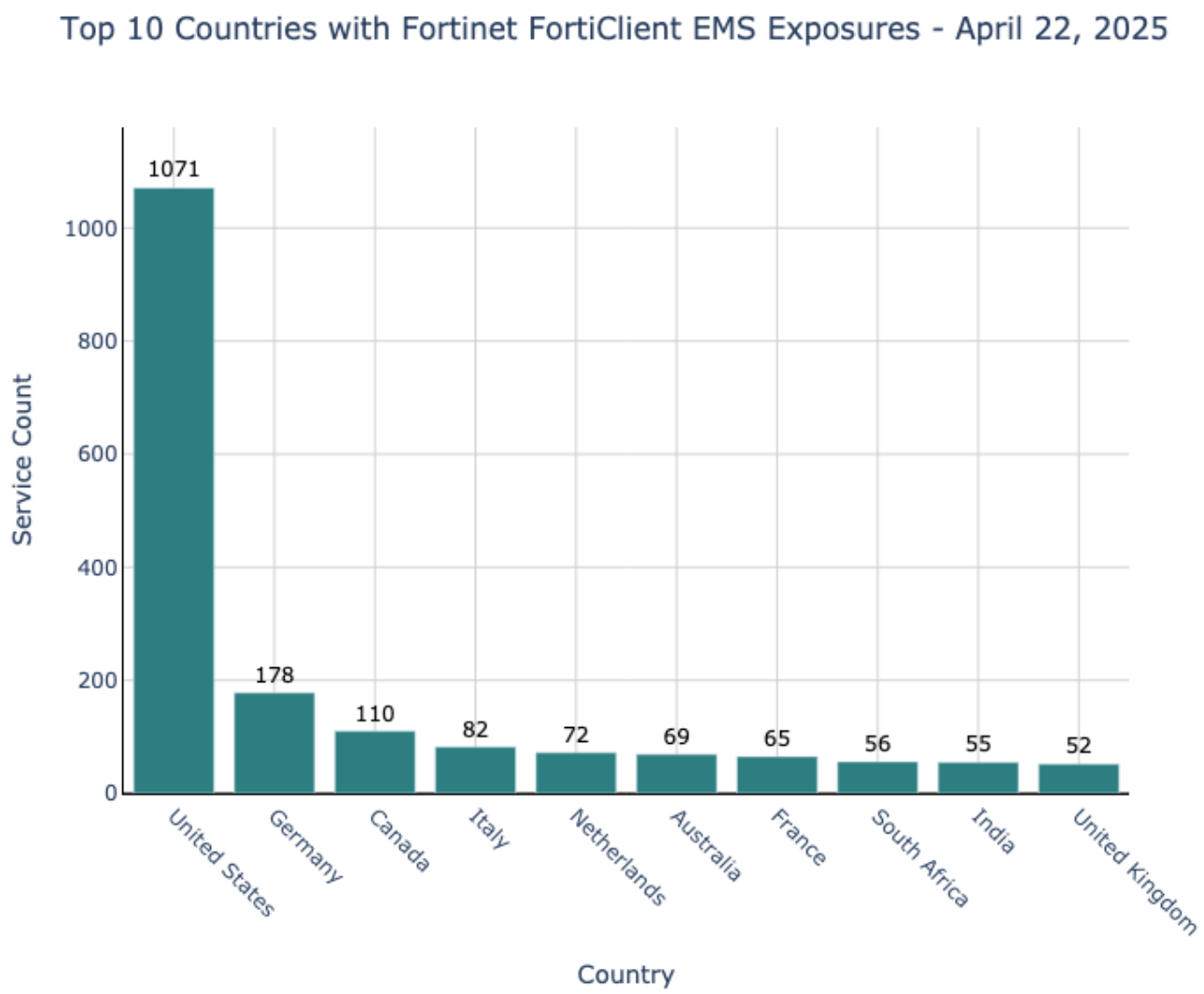
- **CVSS Score: 9.8**
- **Technical Impact: Allows unauthenticated, remote attackers to execute arbitrary SQL queries via specially crafted requests. Successful exploitation can lead to unauthorized access and potential system control.**

This critical vulnerability affects the FortiClient Enterprise Management Server (EMS), a central management solution for enterprise endpoints. FortiGuard's threat intelligence specifically identifies CVE-2023-48788 among the key vulnerabilities exploited by Salt Typhoon, listing it alongside other "Known Infection Vectors" leveraged in their operations targeting infrastructure in the United States, Southeast Asia, and various African countries.

Exposure Snapshot: As of April 2025, Censys observed **2,800** exposed FortiClient EMS instances that may potentially be vulnerable to CVE-2023-48788, with **43** specifically exposing a version that is potentially vulnerable to the exploit. By contrast, we saw **2,888** exposed devices in October 2024.



Over the past six months, exposed instances showed a mild initial rise by nearly 90 instances between October and December 2024, followed by a 14% decline through the end of the year to 2,562 instances by early January 2025, and a subsequent steady increase since. Rather than showing progress toward reducing the attack surface, these fluctuations likely indicate routine infrastructure changes happening as organizations decommission and deploy new potentially vulnerable instances.



As of April 22, 2025, the United States has the highest concentration of FortiClient EMS exposures by far, with 1,071 instances. Other instances are observed sparingly in Europe, Asia, and Africa.

Takeaways

Our six-month analysis paints a concerning picture: despite growing public awareness of Salt Typhoon's activity, there has been little meaningful reduction in exposed, reportedly targeted devices on the public internet—just 25% since October 2024. This decline is largely due to large declines in Sophos Firewall exposures, while most other platforms, including Ivanti and FortiClient EMS, show only minimal change. Somewhat perplexingly, exposures of Cisco IOS XE—one of the platforms that's arguably most clearly linked to Salt Typhoon exploitation—have actually increased, albeit minimally.

Though most exposed devices remain concentrated in the United States, Sophos Firewalls stand out as an exception, with the majority located in Germany—hinting at possible regional differences in threat visibility.

It's entirely possible that some of these instances may be intentional honeypots, as hinted at by sudden spikes in exposure coinciding with vulnerability disclosures, but the broader long-term exposure trends suggest that many organizations are still struggling to reduce their attack surface. It's also clear that there are particularly difficult challenges defenders face in responding to this threat—especially given the combination of limited actionable intelligence, stealthy tactics, and the difficulty of securing widely deployed, internet-facing infrastructure.

It remains challenging to find publicly available, first-party sources for Salt Typhoon IoCs and TTPs. Many of the reports referenced above often cite reports by other authors rather than their own verified telemetry. These reports are still useful, but the lack of primary sources for Salt Typhoon technical indicators has created frustration in an industry that often leans on the maxim “trust, but verify.”

While the vulnerabilities examined above gained additional notoriety through association with Salt Typhoon, they’re notable for another reason: they are all critical or high severity vulnerabilities in commonly targeted edge devices. Even if Salt Typhoon never leveraged these particular vulnerabilities, other threat actors would continue to target these devices as they can be an excellent entry point to enterprise networks.

Even when not directly vulnerable, the ongoing exposure of these devices poses meaningful security risks. Their presence on the public internet broadens the attack surface and offers threat actors like Salt Typhoon continued opportunities for reconnaissance and unauthorized access. For sectors like telecommunications and government—frequent targets in Salt Typhoon campaigns—this underscores the urgent need for proactive monitoring, even among organizations that may not yet recognize themselves as potential targets.

References

- Strengthening America’s Resilience Against the PRC Cyber Threats: https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats
- GreyNoise Observes Active Exploitation of Cisco Vulnerabilities Tied to Salt Typhoon Attacks: https://www.greynoise.io/blog/greynoise-observes-active-exploitation-of-cisco-vulnerabilities-tied-to-salt-typhoon-attacks
- Weathering the storm: In the midst of a Typhoon: https://blog.talosintelligence.com/salt-typhoon-analysis/
- Suspected China-linked hack on US telecoms worst in nation's history, senator says: https://www.reuters.com/business/media-telecom/suspected-china-linked-hack-us-telecoms-worst-nations-history-senator-says-2024-11-22/
- Sweeping Chinese hack of U.S. telecoms firms is 'still going on,' homeland security secretary says: https://www.nbcnews.com/politics/national-security/vast-chinese-hack-eight-us-telecoms-firms-still-going-official-says-rcna181319

- Infographic: A History of Network Device Threats and What Lies Ahead: https://eclypsium.com/blog/infographic-a-history-of-network-device-threats-and-what-lies-ahead/
- Sophos Firewall: Verify if the hotfix for CVE-2022-3236 is applied: https://support.sophos.com/support/s/article/KBA-000008718?language=en_US
- Determine Fix for IOS XE Software Web UI: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-dublin-17121/221128-software-fix-availability-for-cisco-ios.html?
- KB CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways: https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
- Pervasive SQL injection in DAS component: https://www.fortiguard.com/psirt/FG-IR-24-007
- NVD Advisory CVE-2022-3236: https://nvd.nist.gov/vuln/detail/CVE-2022-3236
- NVD Advisory CVE-2023-20198: https://nvd.nist.gov/vuln/detail/CVE-2023-20198
- NVD Advisory CVE-2023-20273: https://nvd.nist.gov/vuln/detail/cve-2023-20273
- NVD Advisory CVE-2023-46805: https://nvd.nist.gov/vuln/detail/CVE-2023-46805
- NVD Advisory CVE-2024-21887: https://nvd.nist.gov/vuln/detail/CVE-2024-21887
- NVD Advisory CVE-2023-48788: https://nvd.nist.gov/vuln/detail/CVE-2023-48788
- Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions: https://www.trendmicro.com/en_us/research/24/k/earth-estries.html
- RedMike (Salt Typhoon) Exploits Vulnerable Cisco Devices of Global Telecommunications Providers: https://www.recordedfuture.com/research/redmike-salt-typhoon-exploits-vulnerable-devices
- December 2024 Security Advisory Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS) (Multiple CVEs): https://forums.ivanti.com/s/article/December-2024-Security-Advisory-Ivanti-Connect-Secure-ICS-and-Ivanti-Policy-Secure-IPS-Multiple-CVEs?language=en_US
- 9X Surge in Ivanti Connect Secure Scanning Activity: https://www.greynoise.io/blog/surge-ivanti-connect-secure-scanning-activity
- Threat Actor - Salt Typhoon: https://www.fortiguard.com/threat-actor/5557/salt-typhoon