Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

8 February 2024

Vulnerabilities

Fortinet warns of new FortiSIEM RCE bugs in confusing disclosure

Bleeping Computer - February 8 2024

Fortinet is warning of two new unpatched patch bypasses for a critical remote code execution vulnerability in FortiSIEM, Fortinet's SIEM solution. Fortinet added the two new vulnerabilities tracked as CVE-2024-23108 and CVE-2024-23109 to the original advisory for the CVE-2023-34992 flaw in a very confusing update.

Critical Cisco bug exposes Expressway gateways to CSRF attacks

Bleeping Computer - February 7 2024

Cisco has patched several vulnerabilities affecting its Expressway Series collaboration gateways, two of them rated as critical severity and exposing vulnerable devices to cross-site request forgery (CSRF) attacks.

VMware Releases Security Advisory for Aria Operations for Networks

CISA Current Activity - February 7 2024

VMware released a security advisory to address multiple vulnerabilities in Aria Operations for Networks. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.

Unveiling Atlassian Confluence Vulnerability CVE-2023-22527: Understanding and Mitigating Remote Code Execution Risks

Trend Micro Research News Perspectives - February 7 2024

In this blog entry, we discuss CVE-2023-22527, a vulnerability in Atlassian Confluence that has a CVSS score of 10 and could allow threat actors to perform remote code execution.

Linux Distros Hit By RCE Vulnerability in Shim Bootloader

Dark Reading - February 7 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

However, not everyone agrees with the NVD's assessment of CVE-2023-40547 being a near-maximum severity bug.

Malware and threat actors

China-linked APT deployed malware in a network of the Dutch Ministry of Defence

Security Affairs - February 7 2024

China-linked APT group breached the Dutch Ministry of Defence last year and installed malware on compromised systems. Dutch Military Intelligence and Security Service (MIVD) and the General Intelligence and Security Service (AIVD) published a joint report warning that a China-linked APT group breached the Dutch Ministry of Defence last year.

US says China's Volt Typhoon is readying destructive cyberattacks

The Register - Security - February 7 2024

The US government today confirmed that China's Volt Typhoon crew comprised "multiple" critical infrastructure org's IT networks, and warned that the state-sponsored hackers are readying "disruptive or destructive cyberattacks" against these targets.

CISA and Partners Release Advisory on PRC-sponsored Volt Typhoon Activity and Supplemental Living Off the Land Guidance

CISA Current Activity - February 7 2024

Today, CISA, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) released a joint Cybersecurity Advisory (CSA), PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure alongside supplemental Joint Guidance: Identifying and Mitigating Living off the Land Techniques.

Chinese hackers fail to rebuild botnet after FBI takedown

Bleeping Computer - February 7 2024

Chinese Volt Typhoon state hackers failed to revive a botnet recently taken down by the FBI, which was previously used in attacks targeting critical infrastructure across the United States. Before KV-botnet's takedown, it allowed the Volt Typhoon threat group (aka Bronze Silhouette) to proxy malicious activity through hundreds of compromised small office/home offices (SOHO) across the U.S. to evade detection.

Midnight Blizzard and Cloudflare-Atlassian Cybersecurity Incidents

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Security Boulevard - RSS - February 7 2024

Learn about the vulnerabilities in major SaaS platforms brought to light from recent cybersecurity incidents.