Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

16 February 2024

Vulnerabilities

Critical Exchange Server zero-day under active exploitation
SC Magazine US - February 15 2024

Attacks exploiting the critical Domain Name System Security Extensions vulnerability, tracked as CVE-2023-50387 and dubbed "KeyTrap," could be deployed against systems leveraging DNSSEC-validating DNS resolvers and facilitate a massive disruption of the internet, SecurityWeek reports.

CISA Releases Seventeen Industrial Control Systems Advisories
CISA Current Activity - February 15 2024

CISA released seventeen Industrial Control Systems (ICS) advisories on February 15, 2024. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS. ICSA-24-046-01 Siemens SCALANCE W1750D ICSA-24-046-02 Siemens SIDIS Prime ICSA-24-046-03 Siemens SIMATIC RTLS Gateways ICSA-24-046-04 Siemens CP343-1 Devices ICSA-24-046-05 Siemens Location Intelligence ICSA-24-046-06 Siemens Unicam FX ICSA-24-046-07 Siemens Tecnomatix Plant Simulation ICSA-24-046-08 Siemens RUGGEDCOM APE1808 ICSA-24-046-09 Siemens SCALANCE SC-600 Family ICSA-24-046-10 Siemens Simcenter Femap ICSA-24-046-11 Siemens SCALANCE XCM-/XRM-300 ICSA-24-046-12 Siemens SIMATIC WinCC, OpenPCS ICSA-24-046-13.

Malware and threat actors

Ransomware ‘M.O.R.E’ Emerges on Dark Web: Threatens Windows, Mac, Linux Users
The Cyber Express - February 16 2024

A new threat has emerged on the dark web, promising to target victims across multiple operating systems. Dubbed M.O.R.E (Multi OS Ransomware Executable), this dark web tool boasts native compatibility with various operating systems, including Windows, Mac...

Feds Disrupt Botnet Used by Russian APT28 Hackers

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Security Boulevard - RSS - February 15 2024

Federal law enforcement kicked Russian state hackers off a botnet comprising at least hundreds of home office and small office routers that had been pulled together by a cybercriminal group and co-opted by the state-sponsored spies.

TinyTurla Next Generation - Turla APT spies on Polish NGOs

MalwareTips.com - February 15 2024

Cisco Talos has identified a new backdoor authored and operated by the Turla APT group, a Russian cyber espionage threat group. This new backdoor we're calling "TinyTurla-NG" (TTNG) is similar to Turla's previously disclosed implant, TinyTurla, in coding style and functionality.

Volt Typhoon Hits Multiple Electric Utilities, Expands Cyber Activity

Dark Reading - February 15 2024

The portion of China's Volt Typhoon advanced persistent threat (APT) that focuses on infiltrating operational technology (OT) networks in critical infrastructure has already performed reconnaissance and enumeration of multiple US-based electric companies, while also targeting electric transmission and distribution organizations in African nations. That's according to OT security specialist Dragos, which found that the OT threat, which it has dubbed "Voltzite," has been "knocking on the door" of compromising physical industrial control systems (ICSes) at electric-sector targets, though so far their incursions have been limited to the IT networks that connect to the OT footprint.