Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

12 January 2024

Vulnerabilities

Two zero-day bugs in Ivanti Connect Secure actively exploited

Security Affairs - January 11 2024

Ivanti revealed that two threat actors are exploiting two zero-day vulnerabilities in its Connect Secure (ICS) and Policy Secure. Software firm Ivanti reported that threat actors are exploiting two zero-day vulnerabilities (CVE-2023-46805, CVE-2024-21887) in Connect Secure (ICS) and Policy Secure to remotely execute arbitrary commands on targeted gateways.

Infoseccers think attackers backed by China are behind Ivanti zero-day exploits

The Register - Security - January 11 2024

Customers currently left patchless while attacks are expected to increase Security experts believe Chinese nation-state attackers are actively exploiting two zero-day vulnerabilities in security products made by Ivanti.

Move Over, APTs: Cybercriminals Now Target Critical Infrastructure Too

Dark Reading - January 11 2024

A "crimewave" of mass exploitation of Zyxel firewall devices has been washing over critical infrastructure in Europe — and Sandworm, the Russian state-sponsored advanced persistent threat (APT) that specializes in such attacks, is behind only part of it.

Juniper Networks Releases Security Bulletin for Junos OS and Junos OS Evolved

CISA Current Activity - January 11 2024

Juniper Networks has released a security advisory to address a vulnerability (CVE-2024-21611) in Junos OS and Junos OS Evolved. A cyber threat actor could exploit this vulnerability to cause a denial-of-service condition. CISA encourages users and administrators to review the Juniper Advisory JSA75752 and apply the necessary updates.

Microsoft's January 2024 Patch Tuesday Addresses 49 Vulnerabilities, Including Two Critical Vulnerabilities

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Security Bloggers Network - January 11 2024

Microsoft's first Patch Tuesday of 2024 has arrived, and it's a significant one. The tech giant has released fixes for a total of 49 vulnerabilities, including 12 remote code execution (RCE) vulnerabilities and two critical vulnerabilities.

UK cyber

China-Linked Volt Typhoon Hackers Possibly Targeting Australian, UK Governments

SecurityWeek RSS Feed - January 11 2024

Chinese APT Volt Typhoon appears engaged in new attacks against government entities in the US, UK, and Australia. The post China-Linked Volt Typhoon Hackers Possibly Targeting Australian, UK Governments appeared first on SecurityWeek.

Malware and threat actors

Medusa Ransomware Turning Your Files into Stone

Unit42 Palo Alto - RSS - January 11 2024

Medusa ransomware gang has not only escalated activities but launched a leak site. We also analyze new TTPS encountered in an incident response case. The post Medusa Ransomware Turning Your Files into Stone appeared first on Unit 42.

Dutch Man Deployed Stuxnet via Water Pump to Disable Iran's Nukes

HackRead - January 11 2024

By Deeba Ahmed Beyond Bush and Obama: Dutch Investigation Uncovers Hidden Secrets of Stuxnet's Billion-Dollar Attack. This is a post from HackRead[.]com Read the original post: Dutch Man Deployed Stuxnet via Water Pump to Disable Iran's Nukes