Scottish Cyber Coordination Centre

Daily threat bulletin

24 January 2025

Vulnerabilities

QNAP fixes six Rsync vulnerabilities in NAS backup, recovery app

BleepingComputer - 23 January 2025 14:30

QNAP has fixed six rsync vulnerabilities that could let attackers gain remote code execution on unpatched Network Attached Storage (NAS) devices. [...]

Cisco addresses a critical privilege escalation bug in Meeting Management

Security Affairs - 23 January 2025 09:17

Cisco addressed a critical flaw in its Meeting Management that could allow it to gain administrator privileges on vulnerable instances. Cisco released security updates to fix a critical flaw, tracked as CVE-2025-20156 (CVSS score of 9.9) affecting its Meeting Management. A remote, authenticated attacker can exploit the vulnerability to gain administrator privileges on affected instances. [...]

Palo Alto Firewalls Found Vulnerable to Secure Boot Bypass and Firmware Exploits

The Hacker News - 23 January 2025 21:43

An exhaustive evaluation of three firewall models from Palo Alto Networks has uncovered a host of known security flaws impacting the devices' firmware as well as misconfigured security features."These weren't obscure, corner-case vulnerabilities," security vendor Eclypsium said in a report shared with The Hacker News."Instead these were very well-known issues that we wouldn't expect to see

SonicWall Learns From Microsoft About Potentially Exploited Zero-Day

SecurityWeek - 23 January 2025 12:20

SonicWall has credited Microsoft for reporting CVE-2025-23006, a critical remote command execution vulnerability possibly exploited in the wild.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation: CVE-2020-11023 JQuery Cross-Site Scripting (XSS) Vulnerability.

Threat actors and malware

Hundreds of fake Reddit sites push Lumma Stealer malware

BleepingComputer - 23 January 2025 15:05

Scottish Cyber Coordination Centre

Hackers are distributing close to 1,000 web pages mimicking Reddit and the WeTransfer file sharing service that lead to downloading the Lumma Stealer malware. [...]

Stealthy 'Magic Packet' malware targets Juniper VPN gateways

BleepingComputer - 23 January 2025 11:26

A malicious campaign has been specifically targeting Juniper edge devices, many acting as VPN gateways, with malware dubbed J-magic that starts a reverse shell only if it detects a "magic packet" in the network traffic. [...]

Chinese threat actors used two advanced exploit chains to hack Ivanti CSA

Security Affairs - 23 January 2025 15:23

US agencies revealed Chinese threat actors used two advanced exploit chains to breach Ivanti Cloud Service Appliances (CSA). The US government's cybersecurity and law enforcement revealed that Chinese threat actors used at least two sophisticated exploit chains to compromise Ivanti Cloud Service Appliances (CSA). A CISA and FBI published a joint advisory warning that Chinese hackers [...]

Beware: Fake CAPTCHA Campaign Spreads Lumma Stealer in Multi-Industry Attacks

The Hacker News - 23 January 2025 21:30

Cybersecurity researchers are calling attention to a new malware campaign that leverages fake CAPTCHA verification checks to deliver the infamous Lumma information stealer."The campaign is global, with Netskope Threat Labs tracking victims targeted in Argentina, Colombia, the United States, the Philippines, and other countries around the world.

QakBot-Linked BC Malware Adds Enhanced Remote Access and Data Gathering Features

The Hacker News - 23 January 2025 16:13

Cybersecurity researchers have disclosed details of a new BackConnect (BC) malware that has been developed by threat actors linked to the infamous QakBot loader."BackConnect is a common feature or module utilized by threat actors to maintain persistence and perform tasks," Walmart's Cyber Intelligence team told The Hacker News.