Scottish Cyber Coordination Centre

Daily Threat Bulletin

9 March 2026

Vulnerabilities

Cisco flags ongoing exploitation of two recently patched Catalyst SD-WAN flaws

Security Affairs - 06 March 2026 16:14

Cisco warns that two recently patched Catalyst SD-WAN flaws, CVE-2026-20128 and CVE-2026-20122, are already being actively exploited in the wild. Cisco warned customers that threat actors are actively exploiting two recently patched Catalyst SD-WAN vulnerabilities, CVE-2026-20128 and CVE-2026-20122.

CISA warns feds to patch iOS flaws exploited in crypto-theft attacks

BleepingComputer - 06 March 2026 11:57

CISA ordered U.S. federal agencies to patch three iOS security flaws targeted in cyberespionage and crypto-theft attacks using the Coruna exploit kit. [...]

Anthropic Claude Opus AI model discovers 22 Firefox bugs

Security Affairs - 09 March 2026 08:10

Anthropic used Claude Opus 4.6 to identify 22 Firefox vulnerabilities, most of which were high severity, all of which were fixed in Firefox 148, released in January 2026. Anthropic discovered 22 security vulnerabilities in Firefox using its Claude Opus 4.6 AI model in January 2026. Mozilla addressed these issues in Firefox 148.

Critical Nginx UI flaw CVE-2026-27944 exposes server backups

Security Affairs - 08 March 2026 20:10

Nginx UI flaw CVE-2026-27944 lets attackers download and decrypt server backups without authentication, exposing sensitive data on public management interfaces. A critical vulnerability in Nginx UI, tracked as CVE-2026-27944 (CVSS score of 9.8), allows attackers to download and decrypt full server backups without authentication.

Hikvision and Rockwell Automation CVSS 9.8 Flaws Added to CISA KEV Catalog

The Hacker News - 06 March 2026 13:00

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Thursday added two security flaws impacting Hikvision and Rockwell Automation products to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.

Threat actors and malware

Hackers abuse .arpa DNS and ipv6 to evade phishing defenses

BleepingComputer - 08 March 2026 11:12

Threat actors are abusing the special-use ".arpa" domain and IPv6 reverse DNS in phishing campaigns that more easily evade domain reputation checks and email security gateways. [...]

Microsoft: Hackers abusing AI at every stage of cyberattacks

BleepingComputer - 07 March 2026 11:15

Microsoft says threat actors are increasingly using artificial intelligence in their operations to accelerate attacks, scale malicious activity, and lower technical barriers across all aspects of a cyberattack. [...]

Massive GitHub malware operation spreads BoryptGrab stealer

Security Affairs - 08 March 2026 14:38

Trend Micro found BoryptGrab stealer spreading through 100+ GitHub repositories, stealing browser data, crypto wallets, system information, and user files. Trend Micro uncovered a campaign distributing the BoryptGrab information stealer through more than 100 GitHub repositories. BoryptGrab is designed to collect browser and cryptocurrency wallet data, system details, and common files.

Iran-linked MuddyWater deploys Dindoor malware against U.S. organizations

Security Affairs - 06 March 2026 21:05

Iran-linked APT MuddyWater targeted U.S. organizations, deploying the new Dindoor backdoor across sectors including banks, airports, and nonprofits.

Multi-Stage VOID#GEIST Malware Delivering XWorm, AsyncRAT, and Xeno RAT

The Hacker News - 06 March 2026 21:03

Cybersecurity researchers have disclosed details of a multi-stage malware campaign that uses batch scripts as a pathway to deliver various encrypted remote access trojan (RATs) payloads that correspond to XWorm, AsyncRAT, and Xeno RAT.

Microsoft spots ClickFix campaign getting users to self-pwn on Windows Terminal

The Register - 06 March 2026 14:37

Crooks tweak familiar copy-paste ruse so that victims run malicious commands themselves A new twist on the long-running ClickFix scam is now tricking Windows users into launching Windows Terminal and pasting malware into it themselves – handing the credential-stealing Lumma infostealer the keys to their browser vault....