Scottish Cyber Coordination Centre

Daily Threat Bulletin

2 March 2026

Vulnerabilities

CISA and Partners Release Guidance for Ongoing Global Exploitation of Cisco SD-WAN Systems

CISA Advisories -

The Cybersecurity and Infrastructure Security Agency (CISA) has added CVE-2026-20127 and CVE-2022-20775 to its Known Exploited Vulnerabilities (KEV) Catalog on Feb. 25, 2026. As a result of the malicious cyber activity and vulnerabilities involving Cisco SD-WAN systems, CISA has outlined requirements for FCEB agencies in Emergency Directive (ED) 26-03 to inventory Cisco SD-WAN systems, update them, and assess compromise. and Cisco Catalyst SD-WAN Vulnerabilities, and implement Cisco's SD-WAN Hardening Guidance.

CVE-2025-64328 exploitation impacts 900 Sangoma FreePBX instances

Security Affairs - 01 March 2026 11:01

About 900 Sangoma FreePBX systems were infected with web shells after attackers exploited a command injection flaw. Hundreds of Sangoma FreePBX instances are still infected with web shells following attacks that began in December 2025.

ClawJacked Flaw Lets Malicious Sites Hijack Local OpenClaw AI Agents via WebSocket

The Hacker News - 28 February 2026 23:51

OpenClaw has fixed a high-severity security issue that, if successfully exploited, could have allowed a malicious website to connect to a locally running artificial intelligence (AI) agent and take over control.

Threat actors and malware

QuickLens Chrome extension steals crypto, shows ClickFix attack

BleepingComputer - 28 February 2026 15:18

A Chrome extension named "QuickLens - Search Screen with Google Lens" has been removed from the Chrome Web Store after it was compromised to push malware and attempt to steal crypto from thousands of users. [...]

CISA warns that RESURGE malware can be dormant on Ivanti devices

BleepingComputer - 27 February 2026 11:57

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has released new details about RESURGE, a malicious implant used in zero-day attacks exploiting CVE-2025-0282 to breach Ivanti Connect Secure devices. [...]

Claude code abused to steal 150GB in cyberattack on Mexican agencies

Security Affairs - 01 March 2026 14:49

Hackers abused Claude Code to build exploits and steal 150GB of data in a cyberattack targeting Mexican government systems. Hackers abused Anthropic's Claude Code AI assistant to develop exploits, create custom tools, and automatically exfiltrate more than 150GB of data in an attack on Mexican government systems, the Israeli cybersecurity firm Gambit Security reports.

Are current AI systems adaptable to new cyber threats

Security Boulevard - 01 March 2026 23:00

How Prepared Are AI Systems Against Emerging Cyber Threats? Can Artificial Intelligence (AI) really keep up with evolving cyber threats? With technology evolves at an unprecedented pace, so do the tactics and techniques employed by cybercriminals. This poses a critical question for cybersecurity experts: Are adaptive AI systems truly equipped to counter these emerging dangers?

Ransomware payments cratered in 2025, but attacks surged to record highs

The Register - 27 February 2026 17:15

Smaller crews piled in as old names splintered and rebranded Ransomware payments cratered in 2025, but it seems like the cybercrooks launching the attacks didn't get the memo.

UK related

UK government's Vulnerability Monitoring System is working - fixes flow far faster

The Register - 02 March 2026 04:27

DNS vulnerabilities are being addressed 84 percent faster in the UK public sector thanks to an automated vulnerability scanning system established as part of a program kicked off early last year.