Scottish Cyber Coordination Centre

Daily Threat Bulletin

9 February 2026

Vulnerabilities

CISA warns of SmarterMail RCE flaw used in ransomware attacks

BleepingComputer - 06 February 2026 13:16

The Cybersecurity & Infrastructure Security Agency (CISA) in the U.S. has issued a warning about CVE-2026-24423, an unauthenticated remote code execution (RCE) flaw in SmarterMail that is used in ransomware attacks. [...]

U.S. CISA adds SmarterTools SmarterMail and React Native Community CLI flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 06 February 2026 10:22

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds SmarterTools SmarterMail and React Native Community CLI flaws to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added SmarterTools SmarterMail and React Native Community CLI flaws to its Known Exploited Vulnerabilities (KEV) catalog.

Claude Opus 4.6 Finds 500+ High-Severity Flaws Across Major Open-Source Libraries

The Hacker News - 06 February 2026 12:19

Artificial intelligence (AI) company Anthropic revealed that its latest large language model (LLM), Claude Opus 4.6, has found more than 500 previously unknown high-severity security flaws in open-source libraries, including Ghostscript, OpenSC, and CGIF.Claude Opus 4.6.

In Other News: Record DDoS, Epstein's Hacker, ESET Product Vulnerabilities

SecurityWeek - 06 February 2026 13:00

Other noteworthy stories that might have slipped under the radar: AT&T and Verizon response to Salt Typhoon, AI agents solve security challenges, man arrested in Poland for DDos Attacks.

Threat actors and malware

New tool blocks imposter attacks disguised as safe commands

BleepingComputer - 08 February 2026 11:26

A new open-source and cross-platform tool called Tirith can detect homoglyph attacks over command-line environments by analyzing URLs in typed commands and stopping their execution. [...]

DKnife Linux toolkit hijacks router traffic to spy, deliver malware

BleepingComputer - 06 February 2026 14:35

A newly discovered toolkit called DKnife has been used since 2019 to hijack traffic at the edge-device level and deliver malware in espionage campaigns. [...]

EDR, Email, and SASE Miss This Entire Class of Browser Attacks

BleepingComputer - 06 February 2026 11:01

Many modern attacks happen entirely inside the browser, leaving little evidence for traditional security tools. Keep Aware shows why EDR, email, and SASE miss browser-only attacks and how visibility changes prevention. [...]

Compromised dYdX npm and PyPI Packages Deliver Wallet Stealers and RAT Malware

The Hacker News - 06 February 2026 15:10

Cybersecurity researchers have discovered a new supply chain attack in which legitimate packages on npm and the Python Package Index (PyPI) repository have been compromised to push malicious versions to facilitate wallet credential theft and remote code execution.

Shai-hulud: The Hidden Cost of Supply Chain Attacks

darkreading - 06 February 2026 17:25

Recent supply chain attacks involving self-propagating worms have spread far, but the damage and long-term impact is hard to quantify.

Living off the AI: The Next Evolution of Attacker Tradecraft

SecurityWeek - 06 February 2026 13:00

Living off the AI isn't a hypothetical but a natural continuation of the tradecraft we've all been defending against, now mapped onto assistants, agents, and MCP.