Scottish Cyber Coordination Centre

Daily Threat Bulletin

10 February 2026

Vulnerabilities

Hackers exploit SolarWinds WHD flaws to deploy DFIR tool in attacks

BleepingComputer - 09 February 2026 16:28

Hackers are now exploiting SolarWinds Web Help Desk (WHD) vulnerabilities to gain code execution rights on exposed systems and deploy legitimate tools, including the Velociraptor forensics tools, for persistence and remote control. [...]

BeyondTrust warns of critical RCE flaw in remote support software

BleepingComputer - 09 February 2026 09:07

BeyondTrust warned customers to patch a critical security flaw in its Remote Support (RS) and Privileged Remote Access (PRA) software that could allow unauthenticated attackers to execute arbitrary code remotely. [...]

Critical Fortinet FortiClientEMS flaw allows remote code execution

Security Affairs - 09 February 2026 21:54

Fortinet warns of a critical FortiClientEMS vulnerability that lets remote attackers run malicious code without logging in. Fortinet issued an urgent advisory to address a critical FortiClientEMS vulnerability, tracked as CVE-2026-21643 (CVSS score of 9.1).

TeamPCP Worm Exploits Cloud Infrastructure to Build Criminal Infrastructure

The Hacker News - 09 February 2026 15:07

Cybersecurity researchers have called attention to a “massive campaign” that has systematically targeted cloud native environments to set up malicious infrastructure for follow-on exploitation.

Flaw in Anthropic Claude Extensions Can Lead to RCE in Google Calendar: LayerX

Security Boulevard - 09 February 2026 16:38

LayerX researchers say that a security in Anthropic’s Claude Desktop Extensions can be exploited to allow threat actors to place a RCE vulnerability into Google Calendar, the latest report to highlight the risks that come with giving AI models with full system privileges unfettered access to sensitive data.

Threat actors and malware

Chinese cyberspies breach Singapore’s four largest telcos

BleepingComputer - 09 February 2026 18:47

The Chinese threat actor tracked as UNC3886 breached Singapore's four largest telecommunication service providers, Singtel, StarHub, M1, and Simba, at least once last year. [...]

European Commission probes cyberattack on mobile device management system

Security Affairs - 09 February 2026 15:00

The European Commission is investigating a cyberattack after detecting signs that its mobile device management system was compromised. The European Commission is investigating a cyberattack on its mobile device management platform after detecting intrusion traces.

Dutch data watchdog snitches on itself after getting caught in Ivanti zero-day attacks

The Register - 09 February 2026 15:50

Staff data belonging to the regulator and judiciary's governing body accessed The Dutch Data Protection Authority (AP) says it was one of the many organizations popped when attackers raced to exploit recent Ivanti vulnerabilities as zero-days....

Ransomware Groups May Pivot Back to Encryption as Data Theft Tactics Falter

SecurityWeek - 09 February 2026 15:38

As only data exfiltration for extortion no longer delivers ROI, ransomware gangs may increasingly encrypting data for additional leverage.