Scottish Cyber Coordination Centre

Daily Threat Bulletin

19 February 2026

Vulnerabilities

Critical Flaws Found in Four VS Code Extensions with Over 125 Million Installs

The Hacker News - 18 February 2026 19:46

Cybersecurity researchers have disclosed multiple security vulnerabilities in four popular Microsoft Visual Studio Code (VS Code) extensions that, if successfully exploited, could allow threat actors to steal local files and execute code remotely.

Notepad++ patches flaw used to hijack update system

Security Affairs - 18 February 2026 20:28

Notepad++ patched a vulnerability that attackers used to hijack its update system and deliver malware to targeted users. Notepad++ fixed a vulnerability that allowed a China-linked APT group to hijack its update mechanism and selectively push malware to chosen targets.

Telegram channels expose rapid weaponization of SmarterMail flaws

BleepingComputer - 18 February 2026 12:27

Underground Telegram channels shared SmarterMail exploit PoCs and stolen admin credentials within days of disclosure. Flare explains how monitoring these communities reveals rapid weaponization of CVE-2026-24423 and CVE-2026-23760 tied to ransomware activity. [...]

China-linked APT weaponized Dell RecoverPoint zero-day since 2024

Security Affairs - 18 February 2026 13:15

A suspected Chinese state-linked group exploited a critical Dell RecoverPoint flaw (CVE-2026-22769) in zero-day attacks starting mid-2024. Mandiant and Google's Threat Intelligence Group (GTIG) reported that a suspected China-linked APT group quietly exploited a critical zero-day flaw in Dell RecoverPoint for Virtual Machines starting in mid-2024.

U.S. CISA adds Google Chromium CSS, Microsoft Windows, TeamT5 ThreatSonar Anti-Ransomware, and Zimbra flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 18 February 2026 11:55

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Google Chromium CSS, Microsoft Windows, TeamT5 ThreatSonar Anti-Ransomware, and Zimbra flaws to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Google Chromium CSS, Microsoft Windows, TeamT5 ThreatSonar Anti-Ransomware, and Zimbra flaws to its Known Exploited Vulnerabilities (KEV) catalog.

Scottish Cyber Coordination Centre

Critical Grandstream VoIP Bug Highlights SMB Security Blind Spot

darkreading - 18 February 2026 22:15

CVE-2026-2329 allows unauthenticated root-level access to SMB phone infrastructure, so attackers can intercept calls, commit toll fraud, and impersonate users.

Critical infra Honeywell CCTVs vulnerable to auth bypass flaw

BleepingComputer - 18 February 2026 16:58

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) is warning of a critical vulnerability in multiple Honeywell CCTV products that allows unauthorized access to feeds or account hijacking. [...]

Threat actors and malware

AI platforms can be abused for stealthy malware communication

BleepingComputer - 18 February 2026 16:18

AI assistants like Grok and Microsoft Copilot with web browsing and URL-fetching capabilities can be abused to intermediate command-and-control (C2) activity. [...]

Keenadu backdoor found preinstalled on Android devices, powers Ad fraud campaign

Security Affairs - 18 February 2026 09:31

Kaspersky uncovered Keenadu, an Android backdoor used for ad fraud that can even take full control of devices. Kaspersky has identified a new Android malware called Keenadu.

Record Number of Ransomware Victims and Groups in 2025

Infosecurity Magazine - 18 February 2026 12:30

Searchlight Cyber reports a 30% annual increase in ransomware victim numbers in 2025

Chinese APT Group Exploits Dell Zero-Day for Two Years

Infosecurity Magazine - 18 February 2026 11:10

Mandiant reveals campaign featuring exploit of a CVSS 10.0 CVE in Dell RecoverPoint for Virtual Machines

Texas sues TP-Link, alleging it allows China to hack into routers

The Record from Recorded Future News - 18 February 2026 18:01