Scottish Cyber Coordination Centre

Daily Threat Bulletin

13 February 2026

Vulnerabilities

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added four new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2024-43468 Microsoft Configuration Manager SQL Injection Vulnerability
CVE-2025-15556 Notepad++ Download of Code Without Integrity Check Vulnerability
CVE-2025-40536 SolarWinds Web Help Desk Security Control Bypass Vulnerability
CVE-2026-20700 Apple Multiple Buffer Overflow Vulnerability

Apple fixed first actively exploited zero-day in 2026

Security Affairs - 12 February 2026 11:50

Apple released updates for iOS, iPadOS, macOS, watchOS, tvOS, and visionOS to address an actively exploited zero-day tracked as CVE-2026-20700. The flaw is a memory corruption issue in Apple's Dynamic Link Editor (dyld).

Critical BeyondTrust RCE flaw now exploited in attacks, patch now

BleepingComputer - 12 February 2026 17:34

A critical pre-authentication remote code execution vulnerability in BeyondTrust Remote Support and Privileged Remote Access appliances is now being exploited in attacks after a PoC was published online.

WordPress plugin with 900k installs vulnerable to critical RCE flaw

BleepingComputer - 12 February 2026 13:09

A critical vulnerability in the WPvivid Backup & Migration plugin for WordPress, installed on more than 900,000 websites, can be exploited to achieve remote code execution by uploading arbitrary files without authentication.

Threat actors and malware

Google Reports State-Backed Hackers Using Gemini AI for Recon and Attack Support

The Hacker News - 13 February 2026 00:27

Google on Thursday said it observed the North Korea-linked threat actor known as UNC2970 using its generative artificial intelligence (AI) model Gemini to conduct reconnaissance on its targets, as various hacking groups continue to weaponize the tool for accelerating various phases of the cyber attack life cycle.

Scottish Cyber Coordination Centre

AMOS infostealer targets macOS through a popular AI app

BleepingComputer - 12 February 2026 10:25

AMOS infostealer is targeting macOS users by abusing popular AI apps and extension marketplaces to harvest credentials. Flare examines how AMOS operates, spreads through AI-driven lures, and feeds the broader stealer-log cybercrime economy.

Lazarus Campaign Plants Malicious Packages in npm and PyPI Ecosystems

The Hacker News - 12 February 2026 23:25

Cybersecurity researchers have discovered a fresh set of malicious packages across npm and the Python Package Index (PyPI) repository linked to a fake recruitment-themed campaign orchestrated by the North Korea-linked Lazarus Group.

World Leaks Ransomware Group Adds Stealthy, Custom Malware 'RustyRocket' to Attacks

Infosecurity Magazine - 12 February 2026 14:30

Accenture Cybersecurity warns over difficult to detect, "sophisticated toolset" being deployed as part of extortion campaigns.