Scottish Cyber Coordination Centre

Daily Threat Bulletin

12 February 2026

Vulnerabilities

Apple Fixes Exploited Zero-Day Affecting iOS, macOS, and Apple Devices

The Hacker News - 12 February 2026 12:09

Apple on Wednesday released iOS, iPadOS, macOS Tahoe, tvOS, watchOS, and visionOS updates to address a zero-day flaw that it said has been exploited in sophisticated cyber attacks. The vulnerability, tracked as CVE-2026-20700 (CVSS score: N/A), has been described as a memory corruption issue in dyld, Apple's Dynamic Link Editor.

Ivanti Patches Endpoint Manager Vulnerabilities Disclosed in October 2025

SecurityWeek - 11 February 2026 13:14

It also fixed a high-severity authentication bypass that could be exploited remotely without authentication to obtain credentials.

Windows 11 Notepad flaw let files execute silently via Markdown links

BleepingComputer - 11 February 2026 19:15

Microsoft has fixed a "remote code execution" vulnerability in Windows 11 Notepad that allowed attackers to execute local or remote programs by tricking users into clicking specially crafted Markdown links, without displaying any Windows security warnings.

Chipmaker Patch Tuesday: Over 80 Vulnerabilities Addressed by Intel and AMD

SecurityWeek - 11 February 2026 12:00

More than two dozen advisories have been published by the chip giants for vulnerabilities found recently in their products.

Threat actors and malware

LummaStealer infections surge after CastleLoader malware campaigns

BleepingComputer - 11 February 2026 13:02

A surge in LummaStealer infections has been observed, driven by social engineering campaigns leveraging the ClickFix technique to deliver the CastleLoader malware.

Scottish Cyber Coordination Centre

Google says hackers are abusing Gemini AI for all attacks stages

BleepingComputer - 12 February 2026 03:00

Google Threat Intelligence Group (GTIG) has published a new report warning about AI model extraction/distillation attacks, in which private-sector firms and researchers use legitimate API access to systematically probe models and replicate their logic and reasoning.

SSHStalker botnet targets Linux servers with legacy exploits and SSH scanning

Security Affairs - 11 February 2026 10:49

A new Linux botnet, SSHStalker, has infected about 7,000 systems using old 2009-era exploits, IRC bots, and mass-scanning malware. Flare researchers uncovered a previously undocumented Linux botnet dubbed SSHStalker, observed via SSH honeypots over two months.

Reynolds ransomware uses BYOVD to disable security before encryption

Security Affairs - 11 February 2026 16:00

Researchers found a new ransomware, named Reynolds, that implements the Bring Your Own Vulnerable Driver (BYOVD) technique to disable security tools and evade detection before encrypting systems.

Crazy ransomware gang abuses employee monitoring tool in attacks

BleepingComputer - 11 February 2026 15:29

A member of the Crazy ransomware gang is abusing legitimate employee monitoring software and the SimpleHelp remote support tool to maintain persistence in corporate networks, evade detection, and prepare for ransomware deployment.