Scottish Cyber Coordination Centre

Daily Threat Bulletin

24 February 2026

Vulnerabilities

Android mental health apps with 14.7M installs filled with security flaws

BleepingComputer - 23 February 2026 18:59

Several mental health mobile apps with millions of downloads on Google Play contain security vulnerabilities that could expose users' sensitive medical information. [...]

Microsoft says bug in classic Outlook hides the mouse pointer

BleepingComputer - 23 February 2026 15:40

Microsoft is investigating a known issue that causes the mouse pointer to disappear in the classic Outlook desktop email client for some users. [...]

Wormable XMRig Campaign Uses BYOVD Exploit and Time-Based Logic Bomb

The Hacker News - 24 February 2026 00:29

Cybersecurity researchers have disclosed details of a new cryptojacking campaign that uses pirated software bundles as lures to deploy a bespoke XMRig miner program on compromised hosts.

Recent RoundCube Webmail Vulnerability Exploited in Attacks

SecurityWeek - 23 February 2026 11:47

Patched in December 2025, the exploited flaw leads to XSS attacks via the animate tags in SVG documents.

Threat actors and malware

Wormable XMRig campaign leverages BYOVD and timed kill switch for stealth

Security Affairs - 23 February 2026 19:36

A wormable cryptojacking campaign spreads via pirated software, using BYOVD and a time-based logic bomb to deploy a custom XMRig miner. Researchers uncovered a wormable cryptojacking campaign that spreads through pirated software bundles to deploy a custom XMRig miner.

CVE-2026-1731 fuels ongoing attacks on BeyondTrust remote access products

Security Affairs - 23 February 2026 13:09

Attackers are exploiting CVE-2026-1731 in BeyondTrust RS and PRA to deploy VShell, gain persistence, move laterally, and control compromised systems. Threat actors are actively

exploiting a recently disclosed critical vulnerability, tracked as CVE-2026-1731 (CVSS score: 9.9), in BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA). The flaw is being used to conduct a wide [...]

AI-powered campaign compromises 600 FortiGate systems worldwide

Security Affairs - 23 February 2026 11:39

A Russian-speaking cybercriminal used commercial generative AI tools to hack over 600 FortiGate devices across 55 countries. Amazon Threat Intelligence reports that a Russian-speaking, financially motivated threat actor used commercial generative AI services to compromise more than 600 FortiGate devices in 55 countries.

Anthropic Says Chinese AI Firms Used 16 Million Claude Queries to Copy Model

The Hacker News - 24 February 2026 12:34

Anthropic on Monday said it identified “industrial-scale campaigns” mounted by three artificial intelligence (AI) companies, DeepSeek, Moonshot AI, and MiniMax, to illegally extract Claude’s capabilities to improve their own models.

APT28 Targeted European Entities Using Webhook-Based Macro Malware

The Hacker News - 24 February 2026 02:11

The Russia-linked state-sponsored threat actor tracked as APT28 has been attributed to a new campaign targeting specific entities in Western and Central Europe.The activity, per S2 Grupo’s LAB52 threat intelligence team, was active between September 2025 and January 2026. It has been codenamed Operation MacroMaze.

Autonomous AI Agents Provide New Class of Supply Chain Attack

SecurityWeek - 23 February 2026 13:30

While this campaign targets crypto wallets and steals money, the methodology has far wider potential that could be used by other attackers.