Scottish Cyber Coordination Centre

Daily Threat Bulletin

2 February 2026

Vulnerabilities

Microsoft fixes Outlook bug blocking access to encrypted emails

BleepingComputer - 30 January 2026 10:48

Microsoft has fixed a known issue that prevented Microsoft 365 customers from opening encrypted emails in classic Outlook after a recent update. [...]

SmarterTools patches critical SmarterMail flaw allowing code execution

Security Affairs - 30 January 2026 12:53

SmarterTools fixed two SmarterMail flaws, including a critical bug (CVE-2026-24423) that could allow arbitrary code execution. SmarterTools fixed two security bugs in its SmarterMail email software, including a critical vulnerability, tracked as CVE-2026-24423 (CVSS score of 9.3) that could let attackers run malicious code on affected systems.

U.S. CISA adds a flaw in Ivanti EPMM to its Known Exploited Vulnerabilities catalog

Security Affairs - 30 January 2026 11:40

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds a flaw in Ivanti EPMM to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added an Ivanti EPMM vulnerability, tracked as CVE-2026-1281 (CVSS score of 9.8), to its Known Exploited Vulnerabilities (KEV) catalog.

Ivanti Patches Exploited EPMM Zero-Days

SecurityWeek - 30 January 2026 09:32

The critical-severity vulnerabilities could allow unauthenticated attackers to execute arbitrary code remotely.

AIs Are Getting Better at Finding and Exploiting Security Vulnerabilities

Schneier on Security - 30 January 2026 16:35

From an Anthropic blog post:In a recent evaluation of AI models' cyber capabilities, current Claude models can now succeed at multistage attacks on networks with dozens of hosts using only standard, open-source tools, instead of the custom tools needed by previous generations. This illustrates how barriers to the use of AI in relatively autonomous cyber workflows are rapidly coming down, and highlights the importance of security fundamentals like promptly patching known vulnerabilities.

Threat actors and malware

Scottish Cyber Coordination Centre

Exposed MongoDB instances still targeted in data extortion attacks

BleepingComputer - 01 February 2026 12:27

A threat actor is targeting exposed MongoDB instances in automated data extortion attacks demanding low ransoms from owners to restore the data. [...]

Open VSX Supply Chain Attack Used Compromised Dev Account to Spread GlassWorm

The Hacker News - 02 February 2026 11:34

Cybersecurity researchers have disclosed details of a supply chain attack targeting the Open VSX Registry in which unidentified threat actors compromised a legitimate developer's resources to push malicious updates to downstream users.

Mandiant Finds ShinyHunters-Style Vishing Attacks Stealing MFA to Breach SaaS Platforms

The Hacker News - 31 January 2026 14:28

Google-owned Mandiant on Friday said it identified an "expansion in threat activity" that uses tradecraft consistent with extortion-themed attacks orchestrated by a financially motivated hacking group known as ShinyHunters.T

Ransomware Without Encryption: Why Pure Exfiltration Attacks Are Surging

Security Magazine - 02 February 2026 04:00

With pure exfiltration, businesses don't realize they're a victim until it's too late.

eScan Antivirus Delivers Malware in Supply Chain Attack

SecurityWeek - 31 January 2026 16:00

Hackers compromised a MicroWorld Technologies update server and fed a malicious file to eScan customers.

Labyrinth Chollima Evolves into Three North Korean Hacking Groups

Infosecurity Magazine - 30 January 2026 16:40

CrowdStrike assessed that two new threat actor groups have spun off from North Korean Labyrinth Chollima hackers

UK related

Dating-app giants investigate incidents after cybercriminals claim to steal data

The Record from Recorded Future News - 30 January 2026 14:55