Scottish Cyber Coordination Centre

Daily Threat Bulletin

6 February 2026

Vulnerabilities

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

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

CVE-2025-11953 React Native Community CLI OS Command Injection Vulnerability

CVE-2026-24423 SmarterTools SmarterMail Missing Authentication for Critical Function Vulnerability

Critical SmarterMail Vulnerability Exploited in Ransomware Attacks

SecurityWeek - 06 February 2026 08:50

The security defect allows unauthenticated attackers to execute arbitrary code remotely via malicious HTTP requests.

Critical n8n Flaw CVE-2026-25049 Enables System Command Execution via Malicious Workflows

The Hacker News - 05 February 2026 12:46

The flaw, tracked as CVE-2026-25049 (CVSS score: 9.4), is the result of inadequate sanitization that bypasses safeguards put in place to address CVE-2025-68613 (CVSS score: 9.9), another critical defect that was patched by n8n in December 2025.

Claude Opus 4.6 Finds 500+ High-Severity Flaws Across Major Open-Source Libraries

The Hacker News - 06 February 2026 12:19

Artificial intelligence (AI) company Anthropic revealed that its latest large language model (LLM), Claude Opus 4.6, has found more than 500 previously unknown high-severity security flaws in open-source libraries, including Ghostscript, OpenSC, and CGIF.

[R1] Nessus Versions 10.10.2 and 10.11.2 Fix Multiple Vulnerabilities

Tenable Product Security Advisories - 05 February 2026 08:13

One of the third-party components (expat) was found to contain vulnerabilities, and updated versions have been made available by the providers. Out of caution and in line with best practice, Tenable has opted to upgrade these components to address the potential impact of the issues.

Scottish Cyber Coordination Centre

Threat actors and malware

Hacker claims theft of data from 700,000 Substack users; Company confirms breach

Security Affairs - 05 February 2026 21:23

Substack confirmed a data breach after a hacker leaked data from nearly 700,000 users, including email addresses and phone numbers. Substack is an online platform for publishing email-based newsletters and blogs, with built-in paid subscriptions and basic analytics.

Infy Hackers Resume Operations with New C2 Servers After Iran Internet Blackout Ends

The Hacker News - 05 February 2026 16:55

The elusive Iranian threat group known as Infy (aka Prince of Persia) has evolved its tactics as part of efforts to hide its tracks, even as it readied new command-and-control (C2) infrastructure coinciding with the end of the widespread internet blackout the regime imposed at the start of January 2026.

Researchers Expose Network of 150 Cloned Law Firm Websites in AI-Powered Scam Campaign

SecurityWeek - 05 February 2026 15:00

Criminals are using AI to clone professional websites at an industrial scale. A new report shows how one AI-powered network grew to 150+ domains by hiding behind Cloudflare and rotating IP ranges.

Ransomware gang uses ISPsystem VMs for stealthy payload delivery

BleepingComputer - 05 February 2026 16:57

Ransomware operators are hosting and delivering malicious payloads at scale by abusing virtual machines (VMs) provisioned by ISPsystem, a legitimate virtual infrastructure management provider.