Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

30 January 2026

Vulnerabilities

Ivanti warns of two EPMM flaws exploited in zero-day attacks

BleepingComputer - 29 January 2026 18:07

Ivanti has disclosed two critical vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM), tracked as CVE-2026-1281 and CVE-2026-1340, that were exploited in zero-day attacks.

SolarWinds Fixes Four Critical Web Help Desk Flaws With Unauthenticated RCE and Auth Bypass

The Hacker News - 29 January 2026 15:30

SolarWinds has released security updates to address multiple security vulnerabilities impacting SolarWinds Web Help Desk, including four critical vulnerabilities that could result in authentication bypass and remote code execution (RCE).

OpenSSL issued security updates to fix 12 flaws, including Remote Code Execution

Security Affairs - 29 January 2026 09:35

OpenSSL issued security updates fixing 12 vulnerabilities in the open-source cryptographic library, including a high-severity remote code execution flaw. Cybersecurity firm Aisle discovered the twelve vulnerabilities.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.
CVE-2026-1281 Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability

Threat actors and malware

Hugging Face abused to spread thousands of Android malware variants

BleepingComputer - 29 January 2026 18:08

A new Android malware campaign is using the Hugging Face platform as a repository for thousands of variations of an APK payload that collects credentials for popular financial and payment services.

Scottish
Cyber
Coordination
Centre

Aisuru botnet sets new record with 31.4 Tbps DDoS attack

BleepingComputer - 29 January 2026 10:55

The Aisuru/Kimwolf botnet launched a new massive distributed denial of service (DDoS) attack in December 2025, peaking at 31.4 Tbps and 200 million requests per second.

New CISA Guidance Targets Insider Threat Risks

Infosecurity Magazine - 29 January 2026 17:00

CISA urges action against insider threats with publication of a new infographic offering strategies to manage risks.

Ransomware Victim Numbers Rise, Despite Drop in Active Extortion Groups

Infosecurity Magazine - 29 January 2026 14:01

Ransomware victims surged in Q4 2025 despite fewer active extortion groups, with data leaks rising 50%, ReliaQuest researchers report.