Scottish Cyber Coordination Centre

Daily Threat Bulletin

12 January 2026

Vulnerabilities

Trend Micro Apex Central RCE Flaw Scores 9.8 CVSS in On-Prem Windows Versions

The Hacker News - 09 January 2026 16:31

Trend Micro has released security updates to address multiple security vulnerabilities impacting on-premise versions of Apex Central for Windows, including a critical bug that could result in arbitrary code execution.The vulnerability, tracked as CVE-2025-69258, carries a CVSS score of 9.8 out of a maximum of 10.0. T

China-linked cybercrims abused VMware ESXi zero-days a year before disclosure

The Register - 09 January 2026 14:28

Huntress analysis suggests VM escape bugs were already weaponized in the wild Chinese-linked cybercriminals were sitting on a working VMware ESXi hypervisor escape kit more than a year before the bugs it relied on were made public....

CISA Closes 10 Emergency Directives as Vulnerability Catalog Takes Over

SecurityWeek - 09 January 2026 14:41

The Emergency Directives were retired because they achieved objectives or targeted vulnerabilities included in the KEV catalog.

Threat actors and malware

BreachForums hacking forum database leaked, exposing 324,000 accounts

BleepingComputer - 10 January 2026 14:17

The latest incarnation of the notorious BreachForums hacking forum has suffered a data breach, with its user database table leaked online. [...]

Hackers target misconfigured proxies to access paid LLM services

BleepingComputer - 09 January 2026 15:56

Threat actors are systematically hunting for misconfigured proxy servers that could provide access to commercial large language model (LLM) services. [...]

FBI Warns North Korean Hackers Using Malicious QR Codes in Spear-Phishing

The Hacker News - 09 January 2026 12:16

The U.S. Federal Bureau of Investigation (FBI) on Thursday released an advisory warning of North Korean state-sponsored threat actors leveraging malicious QR codes in spear-phishing

campaigns targeting entities in the country."As of 2025, Kimsuky actors have targeted think tanks, academic institutions, and both U.S. and foreign government entities with embedded malicious Quick Response (QR)