Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

9 January 2026

Vulnerabilities

VMware ESXi zero-days likely exploited a year before disclosure

BleepingComputer - 08 January 2026 17:27

Chinese-speaking threat actors used a compromised SonicWall VPN appliance to deliver a VMware ESXi exploit toolkit that seems to have been developed more than a year before the targeted vulnerabilities became publicly known. [...]

Public PoC prompts Cisco patch for ISE, ISE-PIC vulnerability

Security Affairs - 08 January 2026 16:04

Cisco addressed a medium-severity vulnerability in ISE and ISE-PIC after a public PoC exploit was disclosed. Cisco addressed a medium-severity vulnerability, tracked as CVE-2026-20029 (CVSS score: 4.9), in Identity Services Engine (ISE) and ISE Passive Identity Connector (ISE-PIC) after a public PoC exploit was disclosed.

U.S. CISA adds HPE OneView and Microsoft Office PowerPoint flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 08 January 2026 11:41

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds HPE OneView and Microsoft Office PowerPoint flaws to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added HPE OneView and Microsoft Office PowerPoint flaws to its Known Exploited Vulnerabilities (KEV) catalog.

Coolify Discloses 11 Critical Flaws Enabling Full Server Compromise on Self-Hosted Instances

The Hacker News - 08 January 2026 16:23

Cybersecurity researchers have disclosed details of multiple critical-severity security flaws affecting Coolify, an open-source, self-hosting platform, that could result in authentication bypass and remote code execution.

Maximum-severity n8n flaw lets randos run your automation server

The Register - 08 January 2026 12:40

Unauthenticated RCE means anyone on the network can seize full control A maximum-severity bug in the popular automation platform n8n has left an estimated 100,000 servers wide open to complete takeover, courtesy of a flaw so bad it doesn’t even require logging in.

Critical Vulnerability Patched in jsPDF

SecurityWeek - 08 January 2026 14:17

The bug can allow attackers to read arbitrary files from the system, potentially exposing configurations and credentials.

Phishing Attacks Exploit Misconfigured Email Routing Settings to Target Microsoft 365 Users

Infosecurity Magazine - 08 January 2026 15:01

Misconfigurations abused to make phishing emails look like they come from within the organization

Threat actors and malware

New China-linked hackers breach telcos using edge device exploits

BleepingComputer - 08 January 2026 19:39

A sophisticated threat actor that uses Linux-based malware to target telecommunications providers has recently broadened its operations to include organizations in Southeastern Europe. [...]

Chinese-speaking hackers exploited ESXi zero-days long before disclosure

Security Affairs - 09 January 2026 01:06

Chinese-speaking attackers used a hacked SonicWall VPN to deploy ESXi zero-days that were likely exploited over a year before public disclosure. Chinese-speaking attackers were seen abusing a hacked SonicWall VPN to deliver a toolkit targeting VMware ESXi.

Yes, criminals are using AI to vibe-code malware

The Register - 08 January 2026 12:00

They also hallucinate when writing ransomware code Interview With everyone from would-be developers to six-year-old kids jumping on the vibe coding bandwagon, it shouldn’t be surprising that criminals like automated coding tools too.

GoBruteforcer Botnet Targets Linux Servers

Infosecurity Magazine - 08 January 2026 18:30

The GoBruteforcer botnet has been observed targeting exposed Linux servers on services like FTP and MySQL

Fake WinRAR downloads hide malware behind a real installer

Malwarebytes - 08 January 2026 11:36

We unpack a trojanized WinRAR download that was hiding the Winzipper malware behind a real installer.

UK related

New Update on Jaguar Land Rover Cyberattack: Q3 Wholesales Down 43%

Security Magazine - 09 January 2026 03:00

6 months after facing a cyberattack, JLR releases an update.

UK Government Unveils New Cyber Action Plan

SecurityWeek - 08 January 2026 17:33

The UK government’s cyber action plan is by the government for the government, and has no advice for the private sector nor CNI.

US To Leave Global Forum on Cyber Expertise

Infosecurity Magazine - 08 January 2026 12:15

The Trump administration decided to leave 66 international organizations, including the GFCE and the European Centre of Excellence for Countering Hybrid Threats