Scottish Cyber Coordination Centre

Daily Threat Bulletin

28 January 2026

Vulnerabilities

Fortinet blocks exploited FortiCloud SSO zero day until patch is ready

BleepingComputer - 27 January 2026 19:19

Fortinet has confirmed a new, actively exploited critical FortiCloud single sign-on (SSO) authentication bypass vulnerability, tracked as CVE-2026-24858, and says it has mitigated the zero-day attacks by blocking FortiCloud SSO connections from devices running vulnerable firmware versions.

Microsoft Office Zero-Day (CVE-2026-21509) - Emergency Patch Issued for Active Exploitation

The Hacker News - 27 January 2026 17:07

The vulnerability, tracked as CVE-2026-21509, carries a CVSS score of 7.8 out of 10.0. It has been described as a security feature bypass in Microsoft Office.

High-Severity Remote Code Execution Vulnerability Patched in OpenSSL

SecurityWeek - 28 January 2026 08:36

A total of 12 vulnerabilities have been fixed in OpenSSL, all discovered by a single cybersecurity firm.

Critical sandbox escape flaw found in popular vm2 NodeJS library

BleepingComputer - 27 January 2026 12:35

A critical-severity vulnerability in the vm2 Node.js sandbox library, tracked as CVE-2026-22709, allows escaping the sandbox and executing arbitrary code on the underlying host system.

Critical Grist-Core Vulnerability Allows RCE Attacks via Spreadsheet Formulas

The Hacker News - 27 January 2026 17:06

A critical security flaw has been disclosed in Grist-Core, an open-source, self-hosted version of the Grist relational spreadsheet-database, that could result in remote code execution. The vulnerability, tracked as CVE-2026-24002 (CVSS score: 9.1), has been codenamed Cellbreak by Cyera Research Labs.

WinRAR path traversal flaw still exploited by numerous hackers

BleepingComputer - 27 January 2026 15:38

Multiple threat actors, both state-sponsored and financially motivated, are exploiting the CVE-2025-8088 high-severity vulnerability in WinRAR for initial access and to deliver various malicious payloads.

Scottish Cyber Coordination Centre

Critical Telnet Server Flaw Exposes Forgotten Attack Surface

darkreading - 27 January 2026 22:00

While telnet is considered obsolete, the network protocol is still used by hundreds of thousands of legacy systems and IoT devices for remote access.

[R1] Tenable Network Monitor Version 6.5.3 Fixes Multiple Vulnerabilities

Tenable Product Security Advisories - 27 January 2026 20:02

Several of the third-party components (libxml2, libxslt, expat, c-ares, curl, sqlite) were found to contain vulnerabilities, and updated versions have been made available by the providers. Nessus Network Monitor version 6.5.3 updates libxml2 to version 2.13.9, libxslt to version 1.1.45, expat to version 2.7.3, c-ares to version 1.34.6, curl to 8.17.0 and sqlite to version 3.49.0.

Threat actors and malware

ClickFix Attacks Expand Using Fake CAPTCHAs, Microsoft Scripts, and Trusted Web Services

The Hacker News - 27 January 2026 21:08

Cybersecurity researchers have disclosed details of a new campaign that combines ClickFix-style fake CAPTCHAs with a signed Microsoft Application Virtualization (App-V) script to distribute an information stealer called Amatera.

Chinese Mustang Panda hackers deploy infostealers via CoolClient backdoor

BleepingComputer - 27 January 2026 18:26

The Chinese espionage threat group Mustang Panda has updated its CoolClient backdoor to a new variant that can steal login data from browsers and monitor the clipboard.

China-Linked Hackers Have Used the PeckBirdy JavaScript C2 Framework Since 2023

The Hacker News - 27 January 2026 15:31

Cybersecurity researchers have discovered a JScript-based command-and-control (C2) framework called PeckBirdy that has been put to use by China-aligned APT actors since 2023 to target multiple environments.

Vibe-Coded ‘Sicarii’ Ransomware Can’t Be Decrypted

darkreading - 27 January 2026 23:15

A new ransomware strain that entered the scene last year has poorly designed code and an odd "Hebrew" identity that might be a false flag.

Scottish Cyber Coordination Centre

WhatsApp Rolls Out Lockdown-Style Security Mode to Protect Targeted Users From Spyware

The Hacker News - 27 January 2026 23:24

The feature, similar to Lockdown Mode in Apple iOS and Advanced Protection in Android, aims to protect individuals, such as journalists or public-facing figures and from sophisticated spyware.

Over 100 Organizations Targeted in ShinyHunters Phishing Campaign

SecurityWeek - 27 January 2026 15:57

Domains set up by the threat actor suggest attacks aimed at Atlassian, Canva, Epic Games, HubSpot, Moderna, ZoomInfo, and WeWork.

UK incidents

China-linked group accused of spying on phones of UK prime ministers' aides – for years

The Register - 27 January 2026 16:50

Chinese state-linked hackers are accused of spending years inside the phones of senior Downing Street officials, exposing private communications at the heart of the UK government.