Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

14 January 2026

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-2026-20805 Microsoft Windows Information Disclosure Vulnerability

Microsoft January 2026 Patch Tuesday fixes 3 zero-days, 114 flaws

BleepingComputer - 13 January 2026 14:34

Today is Microsoft's January 2026 Patch Tuesday with security updates for 114 flaws, including one actively exploited and two publicly disclosed zero-day vulnerabilities.

Adobe Patches Critical Apache Tika Bug in ColdFusion

SecurityWeek - 13 January 2026 20:54

Adobe has released patches for 25 vulnerabilities across its products, including a critical Apache Tika flaw in ColdFusion.

SAP's January 2026 Security Updates Patch Critical Vulnerabilities

SecurityWeek - 13 January 2026 13:20

SAP has released 17 security notes, including four that address critical SQL injection, RCE, and code injection vulnerabilities.

Google confirms Android bug causing volume key issues

BleepingComputer - 13 January 2026 14:25

Google has confirmed a software bug that is preventing volume buttons from working correctly on Android devices with accessibility features enabled.

ServiceNow Patches Critical AI Platform Flaw Allowing Unauthenticated User Impersonation

The Hacker News - 13 January 2026 18:17

ServiceNow has disclosed details of a now-patched critical security flaw impacting its ServiceNow artificial intelligence (AI) Platform that could enable an unauthenticated user to impersonate another user and perform arbitrary actions as that user.

Broadcom Wi-Fi Chipset Flaw Allows Hackers to Disrupt Networks

SecurityWeek - 13 January 2026 15:10

The vulnerability was discovered in Asus routers, but all devices using the affected chipset are susceptible to attacks.

Threat actors and malware

New VoidLink malware framework targets Linux cloud servers

BleepingComputer - 13 January 2026 18:12

A newly discovered advanced cloud-native Linux malware framework named VoidLink focuses on cloud environments, providing attackers with custom loaders, implants, rootkits, and plugins designed for modern infrastructures.

PLUGGYAPE Malware Uses Signal and WhatsApp to Target Ukrainian Defense Forces

The Hacker News - 14 January 2026 12:18

The Computer Emergency Response Team of Ukraine (CERT-UA) has disclosed details of new cyber attacks targeting its defense forces with malware known as PLUGGYAPE between October and December 2025. The activity has been attributed with medium confidence to a Russian hacking group tracked as Void Blizzard (aka Laundry Bear or UAC-0190).

New Malware Campaign Delivers Remcos RAT Through Multi-Stage Windows Attack

The Hacker News - 13 January 2026 15:38

Cybersecurity researchers have disclosed details of a new campaign dubbed SHADOW#REACTOR that employs an evasive multi-stage attack chain to deliver a commercially available remote administration tool called Remcos RAT and establish persistent, covert remote access.

Cyber Insights 2026: External Attack Surface Management

SecurityWeek - 13 January 2026 18:00

AI will assist companies in finding their external attack surface, but it will also assist bad actors in locating and attacking the weak points.