Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

23 January 2026

Vulnerabilities

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added four new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2025-31125 Vite Vitejs Improper Access Control Vulnerability

CVE-2025-34026 Versa Concerto Improper Authentication Vulnerability

CVE-2025-54313 Prettier eslint-config-prettier Embedded Malicious Code Vulnerability

CVE-2025-68645 Synacor Zimbra Collaboration Suite (ZCS) PHP Remote File Inclusion Vulnerability

SmarterMail auth bypass flaw now exploited to hijack admin accounts

BleepingComputer - 22 January 2026 14:44

Hackers began exploiting an authentication bypass vulnerability in SmarterTools' SmarterMail email server and collaboration tool that allows resetting admin passwords.

Cisco Fixes Actively Exploited Zero-Day CVE-2026-20045 in Unified CM and Webex

The Hacker News - 22 January 2026 10:36

Cisco has released fresh patches to address what it described as a "critical" security vulnerability impacting multiple Unified Communications (CM) products and Webex Calling Dedicated Instance that it has been actively exploited as a zero-day in the wild.

Critical GNU InetUtils telnetd Flaw Lets Attackers Bypass Login and Gain Root Access

The Hacker News - 22 January 2026 23:00

The vulnerability, tracked as CVE-2026-24061, is rated 9.8 out of 10.0 on the CVSS scoring system. It affects all versions of GNU InetUtils from version 1.9.3 up to and including version 2.7.

Threat actors and malware

Okta SSO accounts targeted in vishing-based data theft attacks

BleepingComputer - 22 January 2026 17:43

Okta is warning about custom phishing kits built specifically for voice-based social engineering (vishing) attacks. BleepingComputer has learned that these kits are being used in active attacks to steal Okta SSO credentials for data theft.

Automated FortiGate Attacks Exploit FortiCloud SSO to Alter Firewall Configurations

The Hacker News - 22 January 2026 12:25

Cybersecurity company Arctic Wolf has warned of a “new cluster of automated malicious activity” that involves unauthorized firewall configuration changes on Fortinet FortiGate devices.

New Osiris Ransomware Emerges as New Strain Using POORTRY Driver in BYOVD Attack

The Hacker News - 23 January 2026 00:30

Cybersecurity researchers have disclosed details of a new ransomware family called Osiris that targeted a major food service franchisee operator in Southeast Asia in November 2025.

INC ransomware opsec fail allowed data recovery for 12 US orgs

BleepingComputer - 22 January 2026 12:21

An operational security failure allowed researchers to recover data that the INC ransomware gang stole from a dozen U.S. organizations.