



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

23 October 2026

Vulnerabilities

[Amazon says PHP2Shell exploitation began 4 days before patches](#)

BleepingComputer - 22 October 2026 10:09

Security researchers at Amazon Threat Intelligence say attackers began targeting the PHP2Shell flaws four days before security patches were released on Wednesday.

[Arista patches new VeloCloud Orchestrator zero-day exploited in attacks](#)

BleepingComputer - 22 October 2026 14:18

Arista Networks released security updates to patch an actively exploited zero-day vulnerability affecting VeloCloud Orchestrator (VCO) On-Prem deployments.

[GitLab warns of new max severity code execution vulnerability](#)

BleepingComputer - 22 October 2026 08:41

GitLab has released security patches for a maximum-severity Regular Expression Compiler flaw that can let remote attackers run arbitrary code on vulnerable servers.

[Two CVSS 9.0 Linux KSMDB RCE Flaws Disclosed on Public Mailing Lists Before Kernel Fixes](#)

The Hacker News - 22 October 2026 23:31

Linux servers running KSMDB, the kernel's built-in SMB server, are exposed to two publicly reported remote code execution flaws rated 9.0 by Trend Micro's Zero Day Initiative, with no fix yet in the mainline kernel.

[Cisco Patches 34 Vulnerabilities Across Multiple Products](#)

SecurityWeek - 22 October 2026 11:05

Critical-severity security defects could lead to command execution, authentication bypass, and XSS attacks.

[Oracle Patches Over 1,200 Vulnerabilities With October 2026 CPU](#)

SecurityWeek - 22 October 2026 08:38

Nearly 100 vulnerabilities have been assigned a critical severity rating and Fusion Middleware received the most patches.



Scottish
Cyber
Coordination
Centre

Signal Vulnerability Could Keep Calls Alive After Users Hang Up

Security Affairs - 22 October 2026 19:17

A critical Signal flaw could keep calls active after hang-up, exposing microphone or camera. Update to a fixed version immediately. A critical vulnerability, tracked as CVE-2026-113380 (CVSS score 9.3 of 10), in Signal's calling library could allow a malicious caller to interfere with call termination, potentially leaving the victim's microphone and camera active.

Threat actors and malware

FBI and CISA Warn of SafePay Ransomware Attacks on 600 Organizations

Security Affairs - 22 October 2026 07:48

SafePay ransomware has hit 600+ organizations since 2024, using stolen credentials, VPN access and double extortion to pressure victims into paying. CISA, the FBI, the US Secret Service, Germany's Landeskriminalamt Rheinland-Pfalz, and two UK law enforcement agencies jointly published an advisory this week on SafePay.

#StopRansomware: SafePay Ransomware

CISA Advisories -

Executive Summary

This advisory details recent activity by the SafePay ransomware group. SafePay actors have been highly active since August 2024, targeting businesses and critical infrastructure across North America, South America, Europe, and Australia.

Microsoft Links Storm-0940 to ConnectWise Supply Chain Attack

darkreading - 22 October 2026 21:42

The China-linked actor used an AI-enabled penetration-testing tool to automate and accelerate its attack on more than 2,200 tenants.

Railway warns devs to rotate secrets after potential breach

BleepingComputer - 22 October 2026 18:25

Cloud platform Railway published an urgent warning to users after detecting suspicious activity on its systems that store customer environment variables earlier this week.

Machine speed attacks require machine speed detection and response

BleepingComputer - 22 October 2026 11:02

Attackers can steal credentials and begin exfiltrating data within minutes, often before security teams can respond. Exaforce examines real-world attacks involving stolen GitHub tokens, malicious AI installers, and MFA phishing, explaining why faster detection and automated containment are critical.