Scottish Cyber Coordination Centre

Daily Threat Bulletin

28 October 2026

Vulnerabilities

U.S. CISA adds PHP flaws PHP2Shell to its Known Exploited Vulnerabilities catalog

Security Affairs - 27 October 2026 11:39

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds PHP flaws PHP2Shell to its Known Exploited Vulnerabilities catalog.

Tailscale Patches SSH Flaws That Could Let Hacked Devices Gain Root Access on Other Servers

The Hacker News - 28 October 2026 12:50

Tailscale has released version 1.104.4 to fix flaws in its built-in SSH server that could let an attacker reach services and files on other servers that only the root user should be able to touch.

ShinyHunters-Exploited Oracle PeopleSoft Zero-Day Turns Out to Be Three Chained Flaws

The Hacker News - 28 October 2026 12:34

The critical Oracle PeopleSoft bug that ShinyHunters has exploited since May is not one flaw but three chained together, the researchers who reported it said this week.

Microsoft Authenticator Flaw Let Permissionless Android Apps Steal Work Account Tokens

The Hacker News - 27 October 2026 18:39

Microsoft has fixed a flaw in its Authenticator app for Android that let a malicious app with no permissions pose as a trusted Microsoft app, such as Teams, and collect sign-in tokens for a victim's work account.

iOS, macOS 27.2 Patch 286 Bugs; Fix for Exploited Flaw Backported to iOS 18

SecurityWeek - 27 October 2026 12:49

Apple patched 286 vulnerabilities in iOS and macOS 27.2 and brought the fix for an exploited CoreGraphics zero-day to older iPhones.

Attackers Exploit Teams External Chat to Breach Organizations in Under 15 Minutes

Infosecurity Magazine - 27 October 2026 13:30

Arctic Wolf warned that the function enables highly effective social engineering attacks, which lead to incidents such as ransomware.

Scottish Cyber Coordination Centre

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2026-48356 Adobe Commerce and Magento Unrestricted Upload of File with Dangerous Type Vulnerability; CVE-2026-111497 Google Brotli Unchecked Return Value Vulnerability.

Threat actors and malware

The Huntress Tragic Quadrant: Ranking Threats Hitting Businesses Hardest

BleepingComputer - 27 October 2026 11:01

Attackers are increasingly abusing legitimate IT tools, Microsoft 365 sessions, and everyday workflows to compromise businesses without triggering traditional defenses. Huntress Labs ranks the threats hitting organizations hardest, highlighting which attack techniques deserve immediate attention and which remain emerging risks.

CyberStrikeAI Uses 44 AI Agents to Automate Hacking Operations Against Japan Targets

The Hacker News - 28 October 2026 00:56

Cybersecurity researchers have disclosed details of three cyber attacks targeting organizations in Japan in which artificial intelligence (AI) was a key element, either in the driving seat or to assist a human operator.

Attackers Hijack Dahua IP Cameras in Ukraine Using P2P Access and Auth Weaknesses

The Hacker News - 27 October 2026 13:04

The Computer Emergency Response Team of Ukraine (CERT-UA) has issued an alert warning of unauthorized remote access to video surveillance systems manufactured by Dahua.”Cases of compromising IP cameras and DVRs with access to the video stream, changing the device configuration and creating third-party accounts have been recorded,” the State Special Communications Service of Ukraine (SSSCIP)

SBOMs Alone Can’t Reveal the Scope of a Supply Chain Attack

darkreading - 27 October 2026 20:58

A recent Shai-Hulud attack shows defenders need real-time visibility into production code and affected services to respond to supply chain compromises.

Hackers Infect 953 Online Stores With Scanner-Evading Code

Infosecurity Magazine - 27 October 2026 17:00

Attackers have infected 953 online stores with a scanner-evading JavaScript loader since July 2025.

Scottish Cyber Coordination Centre

UK related

Watchdog Urges Police and Fire Service to Improve Cybersecurity

Infosecurity Magazine - 27 October 2026 10:39

UK police forces and fire and rescue services have been urged to strengthen cybersecurity as rising cyber threats outpace current defenses.