Scottish Cyber Coordination Centre

Daily Threat Bulletin

29 October 2026

Vulnerabilities

Attackers Exploit PHP2Shell Flaws in Internet-Exposed Palo Alto Networks Management Interfaces

The Hacker News - 29 October 2026 12:20

Palo Alto Networks on Wednesday warned that threat actors are exploiting the recently patched PHP2Shell vulnerabilities against publicly-accessible management interfaces.

Hackers Start Probing Fresh Oracle EBS Vulnerability

SecurityWeek - 28 October 2026 10:14

CVE-2026-101767 is an unauthenticated SQL injection that can be exploited for remote code execution.

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-2026-41709 Broadcom VMWare ESX Insufficient Logging Vulnerability

CVE-2026-46300 Linux Kernel Missing Initialization of a Variable Vulnerability

InfraTrust report warns of exploited flaws in critical network infrastructure

BleepingComputer - 28 October 2026 11:00

Attackers are actively exploiting vulnerabilities across critical network infrastructure, and PHP flaws known as “PHP2Shell” put the web management interfaces of firewalls, VPNs, application delivery controllers, and other appliances at risk.

CISA warns of hackers now exploiting critical Node2Shell flaw

BleepingComputer - 28 October 2026 07:46

On Tuesday, the US Cybersecurity and Infrastructure Security Agency (CISA) confirmed that hackers have begun exploiting a critical Brotli vulnerability known as Node2Shell, Broccoli2Shell, and HTTP2Shell.

CVE-2026-97631: 16-Year-Old UEFI Flaw Threatens Servers

Security Affairs - 28 October 2026 12:15

CVE-2026-97631: A 16-year-old UEFI flaw (CVSS score of 9.5/10) enables pre-OS code execution. Exposed servers need firmware patches and checks.

Scottish Cyber Coordination Centre

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.

Adobe Fixes 8 Critical Campaign Classic Flaws Allowing Code Execution and Security Bypass

The Hacker News - 28 October 2026 17:45

Adobe has released patches to address multiple critical security flaws in Campaign Classic that, if successfully exploited, could result in arbitrary code execution, security feature bypass, and privilege escalation.

Chrome and Firefox Updates Patch Over 200 Vulnerabilities

SecurityWeek - 28 October 2026 14:39

The Chrome 156 update fixes 52 bugs, while Firefox 159 was rolled out with 167 security patches.

Threat actors and malware

Volt Typhoon hides zero-day attacks using 'Silent Train' framework

BleepingComputer - 28 October 2026 13:00

Chinese state-sponsored hacking group Volt Typhoon has been using a framework that relies on rotating chains of connected devices compromised on demand, including for zero-day attacks targeting high-value systems.

GhostAction Hacking Wave Fizzles, But Attackers Lurk on in GitHub

darkreading - 28 October 2026 20:39

The supply chain attack campaign's shift toward developer endpoints and cloud access signals what could be next for the cybercrime outfit.

Adobe Commerce PolyShell Attacks Breach Hundreds of Stores as Brotli Exploit Traffic Emerges

The Hacker News - 28 October 2026 12:12

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday added two vulnerabilities impacting Adobe Commerce and Magento, and Google's Brotli decoder library to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.

Scottish Cyber Coordination Centre

Three Japan-Focused Cyberattacks Show How Hackers Use AI

Security Affairs - 28 October 2026 09:34

Three Japan-focused cyberattacks show how AI helps hackers scale operations, while exploiting old systems and weak security remains key. In autumn 2026, Japanese companies and other organizations reported a series of data leaks involving their web systems.