Scottish Cyber Coordination Centre

Daily Threat Bulletin

6 November 2026

Vulnerabilities

OpenSSH flaw lets attackers log into password-disabled Linux accounts

BleepingComputer - 05 November 2026 13:45

A newly disclosed OpenSSH vulnerability dubbed “*sshole” allows attackers to log in to certain Alpine Linux and other musl-based Linux accounts that are configured to block password authentication, simply by entering an oversized password.

U.S. CISA adds Apple flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 05 November 2026 09:55

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Apple flaw to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added an Apple flaw, tracked as CVE-2024-27834 (CVSS score of 5.5), to its Known Exploited Vulnerabilities (KEV) catalog.

OpenAI AI Pipeline Generates 948 Linux Root Escalation Exploits in 30-Hour Run

The Hacker News - 05 November 2026 18:38

OpenAI on Wednesday detailed a pipeline that employed an upcoming cyber-focused artificial intelligence (AI) model to validate and patch 948 local privilege escalation vulnerabilities in Linux for $1.2 million in API costs.

Zyxel GS1900 Patch Fails to Block Zero-Day Exploit Allowing Root Command Execution

The Hacker News - 05 November 2026 13:36

Zyxel GS1900 network switches that received the vendor’s earlier fix for an actively exploited flaw are still open to the exploit attackers used, researchers at Binarly found. The exploit lets anyone who can reach a switch’s web management interface run commands on it without logging in.

Cisco, WatchGuard Release Patches; SonicWall Won’t Fix GMS Flaws

SecurityWeek - 05 November 2026 13:33

Cisco patched an RCE in UCS Central Software; WatchGuard fixed authentication and MitM flaws.The post Cisco, WatchGuard Release Patches; SonicWall Won’t Fix GMS Flaws appeared first on SecurityWeek.

Scottish Cyber Coordination Centre

Russia-Linked Hackers Hit iOS, Android Devices With Exploit Chains via Watering Holes

SecurityWeek - 05 November 2026 11:37

The large-scale watering hole campaign has been targeting entities in the US and Europe, mainly in Ukraine.The post Russia-Linked Hackers Hit iOS, Android Devices With Exploit Chains via Watering Holes appeared first on SecurityWeek.

GhostMap Bug Leaves Android Phones Stuck in Reboot Loop

Infosecurity Magazine - 05 November 2026 11:15

Bitdefender warns that unfixed GhostMap bug could force users to factory reset their device.

Threat actors and malware

Hackers backdoor Linux servers using trojanized CWP web server

BleepingComputer - 05 November 2026 12:24

A new Linux malware called CWPdoor is being distributed through a trojanized version of cwpsrv, the web server behind the Control Web Panel (CWP) management interface.

Russian APT29 Targets Mobile Users with Watering Hole Attacks

Security Affairs - 05 November 2026 11:00

Russia-linked group APT29 targeted iOS and Android users through hijacked websites and a compromised analytics service. Sekoia says a large-scale watering hole campaign is going after iOS and Android users, and it links the campaign to APT29 (aka SVR group, Cozy Bear, Nobelium, BlueBravo, Midnight Blizzard, and The Dukes), the Russian group tied to the SVR foreign intelligence service.

APT29's Watering Holes Target Thousands of Mobile Users

darkreading - 05 November 2026 21:05

After compromising websites, the Russian state-sponsored threat group is fingerprinting victims, then harvesting information from the interesting ones.

Zyxel Switch Hacks Blamed on Patched Flaw Actually Exploited a Zero-Day

SecurityWeek - 05 November 2026 11:56

Tracked as CVE-2026-107441, the out-of-bounds write flaw could allow attackers to execute OS commands via crafted HTTP requests.

Chinese Nation-State Threat Activity Falls Sharply in Q2 and Q3 2026

Infosecurity Magazine - 05 November 2026 12:40

Trellix observed a 41.4% drop in China-nexus activity between April and September, which may reflect changing PRC strategic priorities.

Scottish Cyber Coordination Centre

UK related

NATS Air Traffic Control Failure Cost UK Economy £33m

Infosecurity Magazine - 05 November 2026 10:25

Cyber Monitoring Centre report claims an IT failure at the UK's NATS air traffic services provider cost over £30m.