



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

30 October 2026

Vulnerabilities

[CISA warns of Frgnesia Linux flaw chained in PHP2Shell attacks](#)

BleepingComputer - 29 October 2026 10:59

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) warned federal agencies to patch a high-severity Linux kernel privilege escalation bug that attackers are chaining with the PHP2Shell flaws in the wild.

[Hackers exploit Cisco SD-WAN flaw to deploy custom KeyDrift malware](#)

BleepingComputer - 29 October 2026 15:38

A newly identified advanced persistent threat (APT) group tracked as UAT-11473 was observed exploiting CVE-2026-20127, an authentication-bypass flaw in Cisco Catalyst SD-WAN Controllers, to deploy a custom malware framework called KeyDrift.

[Attacker Tried to Exploit Alpine Linux's GitLab via CVSS 10.0 Flaw Its Ruby Left Open](#)

The Hacker News - 29 October 2026 15:35

An attacker tried to exploit a critical GitLab vulnerability on the Alpine Linux project's own GitLab server a week after GitLab released a fix. The flaw, CVE-2026-97229 (CVSS score: 10.0), can let an attacker run code on a GitLab server through a crafted regular expression in a CI configuration.

[Attackers Exploit Second Cisco Firewall VPN Zero-Day Since August](#)

SecurityWeek - 29 October 2026 10:47

An exploited flaw in the Remote Access SSL VPN service lets unauthenticated attackers remotely force ASA and FTD firewalls to reload.

[Adobe, Veeam, Juniper Networks Patch Critical Vulnerabilities](#)

SecurityWeek - 29 October 2026 14:42

The flaws could lead to arbitrary code execution, authorization bypasses, and privilege escalation.



Scottish
Cyber
Coordination
Centre

Threat actors and malware

[Volt Typhoon Used Silent Train to Hide Zero-Day Attacks](#)

Security Affairs - 29 October 2026 11:34

Volt Typhoon used disposable relay chains to hide zero-day attacks on critical systems. Lumen linked Silent Train to at least four zero-days. Lumen's Black Lotus Labs has spent three years tracking a covert network it calls Silent Train, which it ties to Volt Typhoon, the China-linked APT group.

[NIK C2 Malware Can Use Victims' OpenAI Keys for AI Queries](#)

Infosecurity Magazine - 29 October 2026 16:00

NIK C2 malware can fall back on victims' OpenAI API keys to run AI queries

[Anthropic-Themed Phishing Emails Bypass Top Security Tools](#)

darkreading - 29 October 2026 22:21

Obvious phishing emails with numerous red flags are somehow getting past some of the industry-leading secure email gateway (SEG) products.