



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

22 October 2026

Vulnerabilities

Critical Vulnerabilities in PHP Require Immediate Patching

CISA Advisories -

CISA strongly urges organizations to immediately patch the recently disclosed critical vulnerabilities in PHP, CVE-2026-109618 and CVE-2026-109619. These vulnerabilities, known as "php2shell," allow for unauthenticated remote code execution in PHP and affect all PHP installations serving web requests. Organizations should immediately update to PHP 8.5.12, 8.4.27, 8.3.36, or 8.2.35 to fix these vulnerabilities.

CISA: Hackers chain Plex flaws in Plex2Shell attacks to breach servers

BleepingComputer - 21 October 2026 15:34

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) is warning that attackers are actively exploiting four vulnerabilities in Plex Media Server.

Critical GitLab Flaw (CVSS 10.0) Could Allow Unauthenticated RCE Across 12 Years of Releases

The Hacker News - 22 October 2026 01:27

GitLab released fixes on October 21 for a flaw that lets an attacker run code on a self-managed server without logging in, and it affects every version of the software going back to 7.0, released in 2014. The fix matters even for administrators who patched nine days earlier: the October 12 update covered only versions 19.2 and later, and the new fixed versions sit one patch above it.

Threat actors and malware

LiteLLM Compromised in Supply Chain Attack Delivering Credential Stealer and Backdoor

The Hacker News - 22 October 2026 00:31

The popular LiteLLM Python package has been compromised as part of a software supply chain attack that delivered a credential stealer and a backdoor, according to reports from SafeDep, Socket, StepSecurity, and Upwind.

Google Chrome adds Gemini-powered scam detection, warns users of ClickFix attacks

BleepingComputer - 21 October 2026 19:16

Chrome is getting new scam protections that use Gemini to detect deceptive websites and warn users when they copy suspicious commands from ClickFix attacks.

Ransomware Attacks Rise as Rival Gangs Vie For Market Supremacy

Infosecurity Magazine - 21 October 2026 13:00

Cybercriminal groups The Gentlemen and Qilin dominate ransomware attacks - and both are evolving their tactics in an attempt to outdo one another.

China-Linked Hackers Use ARTEX AI Agents in ConnectWise Supply Chain Attack

The Hacker News - 22 October 2026 10:51

Microsoft on Wednesday disclosed that a China state-aligned actor dubbed Storm-0940 was behind the recent supply chain compromise of the ConnectWise Cloud Backup application.

Lazarus hackers use post-quantum cryptography for malware delivery

BleepingComputer - 21 October 2026 17:31

North Korean hackers are using a post-quantum cryptographic mechanism to secure malicious payload delivery in new operations that combine old and new malware.

OVHcloud GitHub Compromise Tied to GlassWorm Threat Actors

darkreading - 21 October 2026 17:50

A developer's GitHub account that was compromised several months earlier was used to push malicious code to unsuspecting users.

New PhaaS Platform Uses AI to Craft Phishing Lures and Mask Malicious Activity

Infosecurity Magazine - 21 October 2026 16:00

Researchers have uncovered Athena StealthRoute, a phishing-as-a-service platform featuring an AI Studio that generates phishing lures and decoy content designed to conceal attacks.

UK incidents

Global scramble to fix critical cyber-security flaws as many websites taken offline

BBC News - 22 October 2026 07:28

Organisations around the world are scrambling to fix a critical cyber-security flaw that could affect millions of websites

Children's Data Stolen After Ransomware Attack Compromises 'Password1' Account

Infosecurity Magazine - 21 October 2026 10:05

The ICO has slammed security failings by the Welsh local government data unit and IT service provider following the 2024 incident