



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

21 October 2026

Vulnerabilities

[PHP warns admins of two critical flaws, emergency patches coming tomorrow](#)

BleepingComputer - 20 October 2026 17:56

The PHP security team is warning administrators to prepare for emergency security updates tomorrow to address two critical vulnerabilities, as information about the flaws has reportedly leaked ahead of their scheduled disclosure.

[Critical FortiSIEM Flaw Gets Public Exploit PoC for Unauthenticated Remote Code Execution](#)

The Hacker News - 20 October 2026 22:08

Cybersecurity researchers have released a proof-of-concept (PoC) exploit for a recently patched critical security flaw impacting Fortinet FortiSIEM that could result in arbitrary code execution.

[ClickFix Attackers Exploit Siemens Software Center Flaw to Deploy Remote Access Trojan](#)

The Hacker News - 20 October 2026 13:41

Siemens has addressed a DLL sideloading vulnerability impacting Siemens Software Center that it said has been exploited in ClickFix attacks.

[PHP2Shell: Mass Exploitation Looms for Leaked Critical PHP Flaws](#)

SecurityWeek - 21 October 2026 08:02

Tracked as CVE-2026-109618 and CVE-2026-109619, the bugs could potentially lead to unauthenticated remote code execution.

[CISA Adds Six Known Exploited Vulnerabilities to Catalog](#)

CISA Advisories -

CISA has added six new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2026-96652 Plex Media Server Server-Side Request Forgery (SSRF) Vulnerability; CVE-2026-96654 Plex Media Server Improper Neutralization of Encoded URI Schemes in a Web Page Vulnerability; CVE-2026-96655 Plex Media Server Server-Side Request Forgery (SSRF) Vulnerability; CVE-2026-96656 Plex Media Server External Control of File Name or Path Vulnerability; CVE-2026-106931 EG Secure Solutions SiteGuard Server Edition OS Command Injection Vulnerability; CVE-2026-110936 Siemens Software Center Uncontrolled Search Path Element Vulnerability.



Scottish
Cyber
Coordination
Centre

Threat actors and malware

Microsoft Treats AI Agents as Insider Threats in New Security Framework

Security Affairs - 20 October 2026 08:44

Microsoft urges organizations to secure AI Agents as insider threats, using dynamic permissions, continuous risk monitoring and automated containment. Microsoft published a detailed blog post explaining how organizations should secure AI agents. Microsoft sees them as a growing insider threat, not just a possible risk in the future.

Qilin and INC Ransomware Groups Exploit Palo Alto Networks Flaw to Bypass MFA

The Hacker News - 20 October 2026 22:02

Palo Alto Networks has disclosed that it's continuing to observe exploitation of a now-patched security flaw impacting PAN-OS and Prisma Access by ransomware actors. The activity relates to CVE-2026-0257 (CVSS score: 7.8), an authentication bypass flaw that could be exploited by bad actors to set up unauthorized VPN connections.

Hackers Hijack Five OVHcloud CLI Releases to Distribute Secret-Stealing Malware

The Hacker News - 20 October 2026 14:51

An attacker used a contributor's GitHub account to replace the download archives on five existing releases of OVHcloud's command-line tool on Monday, October 19. The account had been hijacked, and the new files were a build designed to steal secrets stored on the disk of any machine that runs it, the cloud provider says.

Hackers Use New ROMULUS ClickFix Platform to Deliver LegionLoader and Other Malware

The Hacker News - 20 October 2026 10:35

Cybersecurity researchers have disclosed details of a ClickFix delivery platform called ROMULUS that's being used to distribute malware such as Legion Loader.

AOMEI Backupper Compromised in Short-Burst Supply Chain Campaign

SecurityWeek - 20 October 2026 14:51

Across multiple short compromise windows, users were served a downloader for the ShinyRoad modular backdoor framework. The post AOMEI Backupper Compromised in Short-Burst Supply Chain Campaign appeared first on SecurityWeek.

Microsoft Targets Rogue AI Agents With Dynamic Permissions, Risk Scoring

SecurityWeek - 20 October 2026 12:30

Microsoft says companies should treat AI agents as insiders, and is adding controls that grant access per task and tighten it as an agent's risk rises. The post Microsoft Targets Rogue AI Agents With Dynamic Permissions, Risk Scoring appeared first on SecurityWeek.