



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

22 September 2026

Vulnerabilities

[Meta's Muse AI Agent 0-Day Vulnerability Allows Attackers to Hijack the Tool and Inject Malware](#)

Cyber Security News - 22 September 2026 04:13

A zero-day vulnerability in Meta's Muse AI agent for macOS could allow malware already running under a user account to hijack the assistant, intercept dictated prompts, inject malicious instructions, and steal authentication material.

[WordPress Click2Shell flaw lets hackers execute PHP on the server](#)

BleepingComputer - 21 September 2026 15:23

Technical details and a proof-of-concept exploit have been published for a new WordPress cross-site request forgery (CSRF) vulnerability dubbed 'Click2Shell' that affects the platform's Core component. [...]

[Zyxel and Veeam Flaws Under Active Exploitation With Command and SYSTEM Access](#)

The Hacker News - 22 September 2026 12:01

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added a now-patched security flaw impacting Zyxel GS1900 series switches to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.

[CISA Adds One Known Exploited Vulnerability to Catalog](#)

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2026-7273 Zyxel GS1900 Series Switches Stack-Based Buffer Overflow Vulnerability

[Organizations Warned of 3 Exploited Linux Kernel Vulnerabilities](#)

SecurityWeek - 21 September 2026 10:31

Attackers could exploit the flaws to cause denial-of-service conditions, disclose memory, or modify memory.

Threat actors and malware

[Hackers Impersonate IT Help Desk on Microsoft Teams to Steal Windows Passwords](#)



Scottish
Cyber
Coordination
Centre

Cyber Security News - 22 September 2026 05:46

Hackers are abusing Microsoft Teams chats to impersonate IT help desk staff, trick employees into installing malware or granting remote access, and steal Windows passwords through a fake lock screen.

WordPress Click2Shell flaw lets hackers execute PHP on the server

BleepingComputer - 21 September 2026 15:23

Technical details and a proof-of-concept exploit have been published for a new WordPress cross-site request forgery (CSRF) vulnerability dubbed 'Click2Shell' that affects the platform's Core component. [...]

Cybercriminals Are Hiding New Malware in Torrents for Popular Films

darkreading - 21 September 2026 20:11

Victims have been identified in Africa, including in Kenya and Uganda.

US Proposes AI Incident Alert System in Talks With China, Bessent Says

SecurityWeek - 22 September 2026 03:01

Trump has resisted calls to slow down AI development, saying that would help China catch up to U.S. companies.

Attackers Abuse npm Trusted Publishing in GHAPPIER Campaign

Infosecurity Magazine - 21 September 2026 14:30

CloudSEK linked GHAPPIER to a compromised npm package with valid trusted-publishing provenance