



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

20 October 2026

Vulnerabilities

[Critical Drupal RCE Vulnerability Could Let Attackers Take Over Websites Without Authentication](#)

Cyber Security News - 19 October 2026 19:13

Drupal has released security updates for a critical remote code execution vulnerability that could let attackers take over affected websites without logging in. Tracked as CVE-2026-108097, the flaw affects the Field UI module in Drupal core.

[CC-4873 - Multiple Critical Vulnerabilities in Next.js](#)

NHS Digital - 19 October 2026 15:05

Severity: Medium Out-of-band security update addresses three vulnerabilities that, if exploited, could result in remote code execution or denial-of-service Out-of-band security update addresses three vulnerabilities that, if exploited, could result in remote code execution or denial-of-service Updated:

[CC-4872 - F5 Releases Security Advisory for Critical Vulnerabilities in NGINX Plus and NGINX Open Source](#)

NHS Digital - 19 October 2026 13:53

Severity: Medium The advisory addresses three vulnerabilities that could allow an unauthenticated remote attacker to cause denial-of-service or potentially achieve remote code execution on affected systems

[Microsoft fixes classic Outlook bug that hid Copilot buttons](#)

BleepingComputer - 19 October 2026 09:44

Microsoft has fixed a known issue that removed the Copilot Chat and Copilot buttons in the classic Outlook desktop mail client for some Windows users. [...]

[Unpatched Broadcom Wi-Fi Flaw Lets Attackers in Range Run Code as Root on Routers](#)

The Hacker News - 19 October 2026 12:59

A flaw in Broadcom's Wi-Fi setup software lets an attacker within radio range run code as root on Broadcom-based routers, without the network password or any pairing step, security researcher Quentin Kaiser disclosed on October 16.

Threat actors and malware



Scottish
Cyber
Coordination
Centre

Hackers Using Fake Google Meet Pages to Steal Google Credentials

Cyber Security News - 20 October 2026 08:18

Two websites are hosting fake Google Meet pages designed to steal Google account credentials and carry out phishing involving two-factor authentication (2FA), according to threat intelligence shared on October 20, 2026. The pages imitate a familiar meeting service to make a request for account details look more believable.

Microsoft Says AI Agents Cannot Be Trusted and Could Become Insider Security Threats

Cyber Security News - 19 October 2026 19:04

Microsoft warns organizations to treat AI agents as potential insider risks not because they are automatically malicious, but because they can access company data, apps, and tools and act on that access at high speed.

Hackers Exploit SiteGuard WAF Vulnerability That Could Give Them Full Control of Servers

Cyber Security News - 19 October 2026 13:07

Hackers are exploiting a command injection flaw in SiteGuard Server Edition, a web application firewall installed directly on protected servers.

Hackers hijack AOMEI update servers to secretly spread malware

BleepingComputer - 19 October 2026 16:40

Hackers reportedly compromised AOMEI's servers to distribute malware through a built-in promotional feature in its backup software, briefly tampering with configuration files before restoring them to their original state to hide the attacks. [...]

OpenCode hack exposes API keys amid AI distillation attacks

BleepingComputer - 19 October 2026 14:27

The open-source AI coding project OpenCode has notified a small number of users that API keys they used with external providers were exposed in a security breach. [...]

Attackers Abuse Stolen ConnectWise Application Credentials to Target Microsoft 365

Security Affairs - 19 October 2026 10:32

Attackers stole ConnectWise application credentials to access Microsoft 365 tenants, prompting the company to suspend cloud services. ConnectWise suspended its Cloud Backup service and took both SaaS Security and Cloud Management offline over the weekend after discovering that unknown attackers had obtained unauthorized access to seven of its application identities.

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

The Hacker News - 20 October 2026 10:35



Scottish
Cyber
Coordination
Centre

Cybersecurity researchers have disclosed details of a ClickFix delivery platform called ROMULUS that's being used to distribute malware such as Legion Loader. According to Forescout Research - Vedere Labs,

GhostAction Attackers Plant Credential Stealer Disguised as Font in 94 GitHub Repositories

The Hacker News - 19 October 2026 19:35

The threat actor behind the GhostAction supply chain attack has expanded beyond injecting malicious GitHub Actions workflows into compromised projects to phish open-source developers and deliver a stealer malware disguised within a fake font file.

Fake Web3 Accelerator Uses npm Packages to Spread Malware and Hijack AI Agent Traffic

The Hacker News - 19 October 2026 16:36

A fake Web3 accelerator has been observed pushing information stealers and backdoors to Windows and macOS systems using malicious npm packages under the pretext of offering free artificial intelligence (AI) credits for Anthropic Claude and Google Gemini, coding tools, and security audits.

Unpatched Broadcom Wi-Fi Flaw Lets Attackers in Range Run Code as Root on Routers

The Hacker News - 19 October 2026 12:59

A flaw in Broadcom's Wi-Fi setup software lets an attacker within radio range run code as root on Broadcom-based routers, without the network password or any pairing step, security researcher Quentin Kaiser disclosed on October 16.H

UK related

Security Leaders Discuss BAE Cyberattack

Security Magazine - 19 October 2026 11:00

BAE Systems was hit with a cyberattack that halted production/distribution of bankruptcy notices.