



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

12 October 2026

Vulnerabilities

[Discourse Image Pipeline Exploit Chains JPEG Race, GhostScript and ImageMagick for File Read](#)

Cyber Security News - 12 October 2026 07:43

A Discourse image upload exploit allowed basic users to read server files by chaining a JPEG processing delay, Ghostscript execution, and ImageMagick features. The research also exposed a separate cache poisoning flaw that could run JavaScript for anonymous visitors. Researchers reported both issues in June 2026 and patched them before publication.

[NVIDIA DCGM Exporter Bug Exposes GPU Servers to Resource Exhaustion Attacks](#)

Cyber Security News - 12 October 2026 05:52

NVIDIA patched high-severity flaw CVE-2026-47483 in DCGM Exporter that allows unauthenticated remote attackers to exhaust server resources, crash GPU monitoring, and disrupt AI workloads. DCGM Exporter is a common monitoring tool for GPU servers and Kubernetes clusters. It reads details such as GPU model, temperature, memory use, power draw, errors, and workload activity, then serves [...]

[CC-4865 - Critical Remote Code Execution Vulnerability in Citrix NetScaler](#)

NHS Digital - 09 October 2026 12:00

Severity: High CVE-2026-107406 could allow remote code execution or denial of service on vulnerable NetScaler deployments configured for SAML authentication. CVE-2026-107406 could allow remote code execution or denial of service on vulnerable NetScaler deployments configured for SAML authentication. Updated: 09 Oct 2026

[Max severity SonicWall SMA1000 flaw now exploited in attacks](#)

BleepingComputer - 09 October 2026 09:32

Attackers are exploiting a maximum-severity vulnerability in SonicWall SMA1000 appliances (CVE-2026-102255) that was patched on Tuesday, three days ago. [...]

[Anthropic Cuts Live Internet Access for Internal AI Tests After Claude Exploits Injection Flaws](#)

The Hacker News - 10 October 2026 15:48

Anthropic on Friday said it's cutting off live internet access for all its internal evaluations following the discovery of new incidents in which its artificial intelligence (AI) models exhibited misaligned behavior and targeted real websites.



Scottish
Cyber
Coordination
Centre

Unpatched AhsayCBS Vulnerabilities Exploited in the Wild

SecurityWeek - 09 October 2026 11:23

The flaws, CVE-2026-105133 and CVE-2026-105134, allow attackers to bypass authentication and inject OS commands.

Anthropic Fast-Tracks AI Bug Reports to OSS Maintainers, Taps 11 Firms for OT Security

SecurityWeek - 09 October 2026 09:19

OSS Scanner sends unreviewed, model-generated vulnerability reports to open source maintainers that opt in.

Threat actors and malware

Ransomware Actors Exploiting Palo Alto GlobalProtect Flaw for Stealthy VPN Access

Cyber Security News - 11 October 2026 04:21

Ransomware groups are actively exploiting CVE-2026-0257, an authentication bypass affecting Palo Alto Networks PAN-OS GlobalProtect and Prisma Access. ReliaQuest reports that multiple threat groups, including Qilin and Settra, are using the flaw to create unauthorized VPN sessions and enter internal networks through trusted remote access services.

Hackers abuse Google Ads, Bing redirects to push Claude ClickFix attacks

BleepingComputer - 09 October 2026 17:31

Hackers are abusing legitimate Bing search-result redirects as click URLs in Google search ads to direct users to fake Claude installers that deliver ClickFix attacks. [...]

Bitdefender finds preinstalled Android malware you can't uninstall, seen in 150 countries

Security Affairs - 11 October 2026 15:41

Bitdefender finds Midnight Mimosa, preinstalled Android malware on cheap MediaTek phones that fakes ad clicks, drops apps and builds a proxy botnet. Bitdefender researchers discovered a campaign called Midnight Mimosa involving preinstalled Android malware on low-cost phones from different brands that use MediaTek platforms. T

Attackers Exploit AhsayCBS Flaws to Deploy XMRig Miners Disguised as Microsoft Edge

The Hacker News - 09 October 2026 19:17

Threat actors have been observed exploiting two recently disclosed flaws in the AhsayCBS backup utility to seize control of affected devices and deploy web shells and XMRig cryptocurrency miners.



Scottish
Cyber
Coordination
Centre