



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

16 October 2026

Vulnerabilities

[CC-4869 - Cisco Releases Advisory For Critical Vulnerability in Cisco Async OS Affecting Secure Email Gateway](#)

NHS Digital - 15 October 2026 12:28

Severity: Medium - Successful exploitation of CVE-2026-76519 could allow an unauthenticated remote attacker to write arbitrary files and execute commands with root privileges

[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-2026-21589 Atlassian Multiple Products Files or Directories Accessible to External Parties Vulnerability

[Hackers exploit Collabora RCE flaw to backdoor Nextcloud servers](#)

BleepingComputer - 15 October 2026 17:25

Threat actors are exploiting a critical command execution flaw, now tracked as CVE-2026-110447, in the Collabora Online - Built-in CODE Server app (richdocumentscode) for Nextcloud.

[Palo Alto Networks Patches PAN-OS Zero-Day Exploited for Remote Code Execution](#)

SecurityWeek - 15 October 2026 07:59

The company says it's aware of limited exploitation against customers' firewalls, and it has made IoCs available.

[Drupal Patches Critical Field UI Flaw With Unauthenticated RCE Path via Contributed Modules](#)

The Hacker News - 15 October 2026 18:37

Drupal core has a critical flaw in its Field UI module that could let an attacker run code on the site's server, and fixes were shipped on October 14 in Drupal 11.4.10, 11.3.19, and 10.6.19.

[BeyondTrust patches zero-day exploited in attacks since August](#)

BleepingComputer - 16 October 2026 03:18

BeyondTrust warned customers on Thursday to patch a critical flaw in its Remote Support (RS) that has been exploited in zero-day attacks since late August.



Scottish
Cyber
Coordination
Centre

Threat actors and malware

[PEERSTITCH Malware Deployed via FortiOS Flaw Bypasses Checks on Tagged VPN Sessions](#)

The Hacker News - 16 October 2026 11:29

A suspected advanced threat actor has been observed exploiting a security flaw in Fortinet FortiOS to deliver a previously unreported memory-resident ARM64 malware known as PEERSTITCH.

[Silent Lynx Exploits WinRAR Flaw to Deploy Reverse Shell in CIS Government Attacks](#)

The Hacker News - 15 October 2026 22:30

The threat actor known as Silent Lynx has been attributed to a fresh set of attacks targeting government organizations across the Commonwealth of Independent States (CIS). The activity, observed from June 2025 through August 2026, involves four different infection chains that make use of macro-enabled documents, PS2EXE downloaders, GitHub-hosted PowerShell, and crafted WinRAR archives.

[GhostAction Compromises About 1,900 GitHub Accounts, Targets Over 30,000 Repositories](#)

The Hacker News - 15 October 2026 15:15

The credential-theft campaign known as GhostAction has ramped up, targeting more than 30,000 repositories across 3,000 users and organizations. The spike, according to GitGuardian, was observed on October 8 and 9, 2026.

[New Aoki Infostealer Targets AI Coding Assistant Credentials](#)

Infosecurity Magazine - 15 October 2026 14:00

Symantec warned that Aoki can steal API keys and tokens from a number of popular AI coding assistants, including Claude and Gemini.

UK incidents

[UK Legal Aid Agency hack worse than thought, with stolen records dating back to 1978](#)

The Record from Recorded Future News - 15 October 2026 15:30

A cyberattack on Britain's Legal Aid Agency (LAA) stole far older and broader records than the government previously disclosed, officials said Wednesday.