



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

6 October 2026

Vulnerabilities

[CISA Warns of Citrix NetScaler Vulnerability Actively Exploited in Attacks](#)

Cyber Security News - 05 October 2026 14:44

The U.S. Cybersecurity and Infrastructure Security Agency has added a Citrix NetScaler vulnerability, tracked as CVE-2026-88779, to its Known Exploited Vulnerabilities catalog after confirming active exploitation. The flaw affects Citrix NetScaler ADC (formerly Citrix ADC) and Citrix NetScaler Gateway (formerly Citrix Gateway). CVE-2026-88779 is an improper restriction of operations within the bounds of a memory

[New Dell System Update flaw lets hackers gain root privileges](#)

BleepingComputer - 05 October 2026 11:53

Dell warned customers to patch a critical vulnerability in the System Update (DSU) command-line interface (CLI) deployment tool as soon as possible. [...]

[Anthropic Mythos Found A Bug in Rejetto HFS. Attackers Are Now Exploiting It.](#)

Security Affairs - 05 October 2026 19:15

AI-assisted research uncovered a critical Rejetto HFS flaw that enables authentication bypass and remote code execution, now exploited in the wild.

[Realtek Jungle SDK Exploit Attempts Deliver Cling Botnet With STUN-Based C2](#)

The Hacker News - 05 October 2026 18:16

Threat actors have been observed attempting to exploit a now-patched critical security flaw impacting the Realtek Jungle software development kit (SDK) to deploy a botnet malware called Cling."

[Atlassian warns of critical file access flaw in its datacenter products](#)

The Register - 06 October 2026 07:20

Tells users 'action required' – but maybe don't make that action a Jira ticket, because it has this bug

[Exploitation Hits Rejetto HFS Vulnerability Discovered by AI](#)

SecurityWeek - 05 October 2026 12:00

CVE-2026-61500 allows attackers to recover the session-cookie signing key and gain administrative access and RCE.



Scottish
Cyber
Coordination
Centre

Google Suspends Open-Source Bug Bounty Due to AI Vulnerability Reports

Infosecurity Magazine - 05 October 2026 11:30

Google has paused its Open Source Vulnerability Rewards Program due to a flood of AI submissions

Threat actors and malware

ClickFix Fake CAPTCHA Attack Executes Malware Hidden Inside Browser Cache

Cyber Security News - 05 October 2026 14:02

A new ClickFix campaign is turning a web safety check into a route for malware. Visitors to compromised websites see a fake CAPTCHA or repair message and are told to open the Windows Run dialog, paste copied text, and press Enter. The instruction looks simple, but it makes the victim run the attacker's command.

Microsoft Exchange Flaw Lets Authenticated Attackers Read Other Users' Mailboxes

The Hacker News - 05 October 2026 22:51

Microsoft has released out-of-band security updates to address a high-severity flaw in Microsoft Exchange Server that could allow an attacker to escalate privileges under certain conditions.

New NetScaler Zero-Day Exploited in Targeted Attacks Can Knock SAML Deployments Offline

The Hacker News - 05 October 2026 13:10

Citrix has released security updates for a high-severity security flaw in NetScaler

Need for Speed: AI-Driven Attacks Are Changing Security Strategies

darkreading - 05 October 2026 14:00

AI-powered attacks are fast, relentless, and automated. How security teams can keep up is top of mind, according to the latest Dark Reading reader poll.

UK related

More UK Schools Are Recovering Faster from Cyber Incidents

Infosecurity Magazine - 05 October 2026 10:30

Ofqual study finds growing number of UK schools are bouncing back "immediately" from cyber-attacks