



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

29 September 2026

Vulnerabilities

[Exploitation of vulnerabilities affecting Citrix NetScaler ADC and Citrix NetScaler Gateway](#)

NCSC - 28 September 2026 13:00

The NCSC is urging UK organisations to promptly mitigate vulnerabilities affecting Citrix NetScaler ADC and Gateway, two of which are being actively exploited.

[CC-4859 - Exploitation of Microsoft SharePoint Remote Code Execution Vulnerability CVE-2026-65660](#)

NHS Digital - 28 September 2026 13:55

Severity: Medium Exploitation of CVE-2026-65660 could allow an authenticated attacker with low-level access to an affected server the ability to execute code on the server Exploitation of CVE-2026-65660 could allow an authenticated attacker with low-level access to an affected server the ability to execute code on the server Updated: 28 Sep 2026

[Official MCP Python SDK Flaw Can Let Malicious Servers Steal OAuth Credentials](#)

The Hacker News - 29 September 2026 12:38

A malicious MCP server could trick an application built on the official MCP Python SDK into handing over the OAuth credentials it uses to log in to a real service, the SDK's maintainers said in a security advisory. Affected versions sent the client secret, the authorization code, and the PKCE proof key to a token endpoint the attacker controlled.

[Critical Apple Zero-Day Vulnerability Actively Exploited in Attacks](#)

Cyber Security News - 29 September 2026 07:34

Apple has released iOS 26.7.1 and iPadOS 26.7.1 to fix a critical zero-day vulnerability that it says may have been exploited in an extremely sophisticated attack against specifically targeted individuals. The security issue, tracked as CVE-2026-86950, affects the CoreGraphics framework, a fundamental Apple component responsible for rendering graphics, images, and documents across iPhones and iPads. [...]

Threat actors and malware

[Pentagon Data Breach – Hackers Reportedly Accessed 3 Million People's Sensitive Data](#)

Cyber Security News - 29 September 2026 05:09

The Pentagon has confirmed a major data breach involving a Defense Manpower Data Center (DMDC) information system, exposing sensitive personal information belonging to more than three million people.

New File Notification Attack Lets Hackers Track User Activity Across Linux, Windows and macOS

Cyber Security News - 28 September 2026 15:33

A cross-platform side-channel attack that abuses file-notification services to monitor user activity on Linux, Windows and macOS. The technique turns inotify, ReadDirectoryChangesW, and FSEvents, which alert applications when files are changed, into a surveillance mechanism requiring no elevated privileges. The study, "File Notification Attacks: Templating and Exploiting Side-Channel Leakage from the File-Notification Systems on Linux, [...]"

AI Accounts Are Becoming the New Target for Infostealers

Security Affairs - 28 September 2026 21:14

Infostealers are exposing corporate AI accounts, sessions and API keys, giving attackers access to sensitive data, compute and connected systems. SOCRadar analyzed stealer log data from the last 90 days and found 482 companies with exposed AI accounts and credentials. Of those, 295 appeared in active logs during that period, suggesting the exposure is recent [...]

Hackers Use NeedyMantis to Maintain Long-Term Access in Breached Networks

The Hacker News - 29 September 2026 01:05

Hackers have used a malware family called NeedyMantis to maintain long-term access to networks they had already breached, Microsoft said in a technical analysis. The malware has been seen in a small number of targeted intrusions at telecommunications organizations, universities, medical nonprofits, intergovernmental organizations, and government contractors

JadePuffer AI Actor Compromises Azure Tenant in Destructive Cloud Attack

darkreading - 28 September 2026 16:33

The "agentic threat actor" may have used exposed credentials to access resources and delete cloud-based storage, applications, and databases.

UK related

NCSC Urges UK organizations to Patch for Citrix NetScaler ADC and Gateway 0-Day Vulnerabilities

Cyber Security News - 28 September 2026 15:56

The UK National Cyber Security Center (NCSC) has urged organizations to take immediate action against eight vulnerabilities affecting customer-managed Citrix NetScaler ADC and NetScaler Gateway appliances. Two critical flaws, CVE-2026-88771 and CVE-2026-88772, are already being exploited against unmitigated systems, turning routine patching into an



Scottish
Cyber
Coordination
Centre

urgent incident-response task. Citrix NetScaler 0-Day Vulnerabilities Citrix's CTX697096
bulletin rates [...]