



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

30 September 2026

Vulnerabilities

[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.

[Amazon Bedrock AgentCore Flaws Could Expose AWS Credentials](#)

Infosecurity Magazine - 29 September 2026 15:00

AWS AgentCore SDK flaws could let attackers run commands in AI sandboxes and reach AWS credentials.

[Update your iPhone, iPad, or Mac: Flaw could run attackers' code](#)

Malwarebytes - 29 September 2026 11:35

A malicious file could trigger the vulnerability. Apple says it may already have been used against iPhone users.

[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-2026-86950 Apple Multiple Products Out-of-Bounds Write Vulnerability.

Threat actors and malware

[Hackers exploit Citrix NetScaler zero-day to deploy web shells](#)

BleepingComputer - 29 September 2026 15:37

Cybersecurity firms say attackers exploited the Citrix NetScaler CVE-2026-88772 zero-day to deploy custom web shells and tunneling malware, gain root access, steal credentials, and spread into internal networks.

[New Spectre v2 attack variant leaks Linux root password hash in minutes](#)

BleepingComputer - 29 September 2026 14:10

A new Branch Target Reuse (BTR) attack has been devised that can recover root password hashes on Intel computers running Linux in 3-5 minutes on average.



Scottish
Cyber
Coordination
Centre

Russia's Star Blizzard Targets 100+ Organizations With Fake Event Invites to Deliver Backdoor

The Hacker News - 29 September 2026 23:50

Russian state hackers known as Star Blizzard have been using fake event invitations to trick people into installing a backdoor on their Windows computers, according to Microsoft.

Apple Zero-Day Vulnerability Weaponized in Targeted Attacks

darkreading - 29 September 2026 22:31

Attackers are exploiting CVE-2026-86950, an out-of-bounds write flaw, in an extremely sophisticated fashion, according to Apple.

RatHat's Evolving C2 Panel Points to Malware-as-a-Service Model

Infosecurity Magazine - 29 September 2026 15:30

RatHat's C2 panel now builds malware and ranks victims with AI across nearly 100 deployments.