



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

25 September 2026

Vulnerabilities

[Cloudflare Containers Vulnerability Could Leak Data Between Customer Workloads](#)

Cyber Security News - 25 September 2026 04:13

Cloudflare has patched a cross-tenant data exposure vulnerability in its Containers platform across its global, multi-tenant cloud computing infrastructure that could allow one customer's workload to recover residual disk data left by another tenant on the same physical host.

[WSO2 and Adobe Commerce Flaws Exploited in Attacks, Added to CISA KEV](#)

The Hacker News - 25 September 2026 11:16

The U.S. Cybersecurity and Infrastructure Security Agency (CISA), on Thursday, added two critical security flaws impacting WSO2 and Adobe Commerce and Magento to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation.

[Unpatched OnePlus Flaws Let Installed Android Apps Gain Root Without Permissions](#)

The Hacker News - 25 September 2026 00:40

A OnePlus 15 running the latest OxygenOS can be rooted by a malicious app the owner installs, one that asks for no special permissions.

[Attackers Exploit WordPress CVE-2026-87902 Within Hours of Disclosure](#)

The Hacker News - 24 September 2026 12:06

Threat actors have begun to actively exploit a critical security flaw in WordPress within hours of public disclosure.

[Salesforce Agentforce vulns allowed 0-click CRM data theft, anonymous phishing](#)

The Register - 24 September 2026 22:01

'SalesBleed' security flaws 'lead to very unexpected consequences'

[Decades-old file security flaws found in Android, Linux, macOS, and Windows](#)

The Register - 24 September 2026 20:00

Security researchers report that Microsoft considers the side-channel leak of file events to be by design

[SolarWinds Patches Critical RCE Flaws in Observability Self-Hosted](#)

SecurityWeek - 24 September 2026 11:40

The vulnerabilities, tracked as CVE-2026-28324 and CVE-2026-28325, can be exploited without authentication.

Threat actors and malware

AvisLoader Windows Malware That Learned to Survive Even After Its Servers Are Taken Down

Cyber Security News - 24 September 2026 13:07

AvisLoader is a Windows malware loader built to keep taking instructions after server takedowns. That makes it difficult to disrupt by simply removing a malicious website..

Microsoft Rebuilds the SOC with AI Agents, SIEM Integration and Machine-Speed Defense

Cyber Security News - 24 September 2026 12:12

Cyberattacks can move faster than a security team can investigate them. Attackers increasingly use AI agents to automate steps that once needed several people, while defenders still work across separate monitoring and protection tools.

Hackers now exploit critical Roundcube flaw in code injection attacks

BleepingComputer - 24 September 2026 10:27

A high-severity Roundcube Webmail vulnerability patched in May is now being actively exploited in attacks, according to the Canadian Centre for Cyber Security. [...]

WSO2 and Adobe Commerce Flaws Exploited in Attacks, Added to CISA KEV

The Hacker News - 25 September 2026 11:16

The U.S. Cybersecurity and Infrastructure Security Agency (CISA), on Thursday, added two critical security flaws impacting WSO2 and Adobe Commerce and Magento to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation.

17,000 URLs Reveal How ClickFix Turns Trusted Websites Into Malware Traps: Report by CTM360

The Hacker News - 24 September 2026 15:44

ClickFix has become the most common way attackers get into enterprise networks, and it does it without an exploit, an attachment, or a file on disk.