

Daily Threat Bulletin

28 September 2026

Vulnerabilities

[Kiteworks urges 6-hour server shutdown over potential zero-day attacks](#)

Bleeping Computer - 25 September 2026 17:41

Secure file-sharing software company Kiteworks is urging customers worldwide to temporarily shut down their servers on Saturday for a six-hour window after receiving threat intelligence warning of a potentially imminent cyberattack.

[Elementor WordPress flaw lets attackers create admin accounts](#)

Bleeping Computer - 25 September 2026 14:13

A cross-site request forgery (CSRF) vulnerability in the Elementor plugin for WordPress could allow an unauthenticated attacker to create administrator accounts.

[CISA warns of Sharepoint, WSO2, Adobe Commerce flaws exploited in attacks](#)

Bleeping Computer - 25 September 2026 13:24

The Cybersecurity and Infrastructure Security Agency (CISA) warns that hackers are exploiting a critical authentication bypass vulnerability (CVE-2026-5430) affecting multiple products from enterprise software provider WSO2.

[Zero-Click Vulnerabilities in Salesforce Agentforce Expose Wider AI Agent Risk](#)

Infosecurity Magazine - 25 September 2026 13:30

The 'SalesBleed' set of weaknesses in Salesforce's Agentforce agents exposed CRM data to attackers via prompt injection and DNS exfiltration

[Roundcube Webmail Vulnerability in Attackers' Crosshairs](#)

Security Week - 25 September 2026 06:57

Tracked as CVE-2026-48842, the exploited bug is an SQL injection that can be exploited without authentication.

Threat actors and malware

[ShinyHunters hacked Clop leak site using Grav CMS path traversal flaw](#)

Bleeping Computer - 25 September 2026 16:57

The Clop ransomware gang has moved its data leak site to a new Tor address after confirming its previous server was compromised and defaced through an unpatched Grav CMS flaw that BleepingComputer has learned is an unauthenticated path traversal vulnerability.



Scottish
Cyber
Coordination
Centre

MacSync malware uses public iCloud calendars to deliver new payloads

Bleeping Computer - 24 September 2026 16:53

A new variant of the MacSync malware targeting macOS systems now uses public iCloud calendar events to deliver new native payloads.

Emerging Ransomware Gang Uses Backup Destruction Threats to Pressure Victims

Infosecurity Magazine - 24 September 2026 15:00

Ransom notes by n0n ransomware claim to take double extortion to a new level of danger for victims.

UK related

Cyber attack on police force may have 'compromised' staff information

BBC - 25 September 2026 15:49

Dyfed-Powys Police says no personal data relating to the public was believed to have been accessed.