Scottish Cyber Coordination Centre

Daily Threat Bulletin

25 May 2026

Vulnerabilities

Ghost CMS SQL injection flaw exploited in large-scale ClickFix campaign

BleepingComputer - 24 May 2026 11:12

A large-scale campaign is exploiting a critical SQL injection vulnerability (CVE-2026-26980) in Ghost CMS to inject malicious JavaScript code that triggers ClickFix attack flows.

Anthropic's Project Glasswing: 10,000+ Vulnerabilities Found in One Month, and the Patching Problem Has Never Been More Obvious

Security Affairs - 24 May 2026 10:07

Anthropic said its AI Project Glasswing found over 10,000 serious vulnerabilities in one month, exposing a growing patching gap.

U.S. CISA adds a flaw in Drupal Core to its Known Exploited Vulnerabilities catalog

Security Affairs - 24 May 2026 08:54

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds a flaw in Drupal Core to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a flaw in Microsoft Exchange Server, tracked as CVE-2026-9082 (CVSS score of 9.8), to its Known Exploited Vulnerabilities (KEV) catalog.

Threat actors and malware

FBI Warns of Kali365 Phishing-as-a-Service Platform After April Microsoft 365 Attacks

Security Boulevard - 24 May 2026 15:16

The FBI issued an advisory on Thursday about Kali365, a Telegram-based phishing-as-a-service platform first observed in April 2026 that enables cybercriminals to capture OAuth tokens and gain persistent access to Microsoft 365 accounts without stealing passwords or bypassing MFA through credential interception. Multiple cybersecurity firms reported hundreds of attacks enabled by the platform.

Ukraine Probes Teen Suspect in Cyber Theft Scheme Targeting California Online Shoppers

Security Boulevard - 24 May 2026 15:12

Ukrainian authorities have identified an 18-year-old suspect from Odesa allegedly linked to an international cybercrime operation that compromised nearly 30,000 customer accounts belonging to an unnamed California-based online retailer between 2024 and 2025.

Scottish Cyber Coordination Centre

UK related

Secure configuration management and environment isolation for UK SMEs

Security Boulevard - 24 May 2026 14:27

For many UK SMEs, software risk does not usually start with a dramatic failure. It starts with small, ordinary mistakes: a setting left on, a test account reused in production, a cloud service exposed more widely than intended, or a deployment that behaves differently in each environment.