Scottish Cyber Coordination Centre

# Daily Threat Bulletin

26 May 2026

## Vulnerabilities

### Ghost CMS flaw abused to push ClickFix attacks on hundreds of sites

Security Affairs - 25 May 2026 19:07

Attackers are exploiting the patched Ghost CMS flaw CVE-2026-26980, compromising over 700 unpatched sites, including universities. Threat actors are actively exploiting a security flaw, tracked as CVE-2026-26980, in Ghost CMS that was fixed months ago in real attacks against unpatched websites.

### Ghost CMS CVE-2026-26980 Exploited to Hijack 700+ Sites for ClickFix Attacks

The Hacker News - 25 May 2026 18:32

Threat actors are exploiting a recently disclosed critical security flaw in Ghost CMS to inject malicious JavaScript code with an aim to fuel ClickFix attacks. According to QiAnXin XLab, the activity involves the exploitation of CVE-2026-26980 (CVSS score: 9.4), an SQL injection vulnerability in Ghost's Content API that could allow an unauthenticated attacker to read arbitrary data.

### 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-2026-9082 Drupal Core SQL Injection Vulnerability.

## Threat actors and malware

### FBI warns of Kali365 phishing service targeting Microsoft 365 accounts

BleepingComputer - 25 May 2026 09:45

The FBI is warning about the Kali365 phishing-as-a-service platform (PhaaS) that is used to hijack Microsoft 365 accounts by abusing OAuth device code authentication to steal session tokens and bypass multi-factor authentication (MFA). [...]

### TrapDoor Supply Chain Attack Spreads Credential-Stealing Malware via npm, PyPI, and CratesIO

The Hacker News - 25 May 2026 12:29

A new coordinated cross-ecosystem software supply chain attack campaign has targeted npm, PyPI, and Crates.io to distribute credential-stealing malware.The campaign, codenamed TrapDoor, spans more than 34 malicious packages across over 384 versions.

Scottish Cyber Coordination Centre

## Laravel-Lang Packages Poisoned for Malware Delivery

SecurityWeek - 25 May 2026 11:41

Published within a 15-minute window, the malicious tags introduced backdoors to exfiltrate CI secrets.

## Over 5,500 GitHub Repositories Infected in 'Megalodon' Supply Chain Attack

SecurityWeek - 25 May 2026 08:40

Fake automated commits injected GitHub Actions workflows containing payloads to steal credentials, CI secrets, keys, and tokens.