Scottish Cyber Coordination Centre

Daily Threat Bulletin

18 August 2026

Vulnerabilities

Microsoft working on Defender patch for ShieldBreak zero-day

Bleeping Computer - 17 August 2026 05:05

Microsoft is working on a security patch for the “ShieldBreak” zero-day vulnerability disclosed last week by security researcher “Nightmare Eclipse” and now tracked as CVE-2026-69414. [...]

Critical GitLab GraphQL Flaw Could Let Unauthenticated Attackers Delete Public Projects

The Hacker News - 18 August 2026 02:33

GitLab has released security updates to address a critical vulnerability impacting its Community Edition (CE) and Enterprise Edition (EE) software that, under certain conditions, could allow an unauthenticated attacker to remotely modify or delete public projects and user data.

Snowflake GitHub Actions Flaw Lets Crafted Issues Trigger Command Injection

The Hacker News - 18 August 2026 00:14

Cybersecurity researchers at Wiz have disclosed a new GitHub Actions workflow injection vulnerability in Snowflake’s public snowflakedb/snowflake-connector-net repository that it said could be exploited through a crafted GitHub issue to execute commands in a workflow containing internal Jira credentials.

Forminator WordPress Flaw Can Enable Unauthenticated RCE via Malicious PHP Uploads

The Hacker News - 17 August 2026 23:52

A critical security flaw has been disclosed in Forminator Forms, a WordPress plugin with more than 600,000 active installations, that could be exploited to achieve arbitrary code execution on susceptible sites.The vulnerability, tracked as CVE-2026-15748, is rated 9.8 out of 10.0 on the CVSS scoring system.

Roundcube 1.6.18 and 1.7.3 Released With Fix for RCE and SSRF Vulnerabilities

Cyber Security News - 17 August 2026 11:24

Roundcube has released versions 1.6.18 and 1.7.3 to address eleven security vulnerabilities affecting its webmail platform. The updates fix a remote code execution flaw, server-side request forgery bypasses, injection vulnerabilities, and stored cross-site scripting issues. Administrators using Roundcube 1.6.x or 1.7.x should update as soon as possible.

Scottish Cyber Coordination Centre

Threat actors and malware

Unisoc VoLTE Video Call Exploit Chain Can Give Attackers Full Android Kernel Access

The Hacker News - 17 August 2026 16:22

Security researchers at SSD Secure Disclosure have published a two-stage exploit chain that achieves full Android kernel access on devices running Unisoc modem firmware through a VoLTE video call, with no fix from the chipset maker.

Evooo1Bot Linux Botnet Exploits Known Flaws to Turn Edge Devices Into SOCKS5 Proxies

The Hacker News - 17 August 2026 14:59

Cybersecurity researchers have flagged a previously undocumented Linux botnet family dubbed Evooo1Bot that derives its core functionality from the Mirai botnet source code and is equipped to turn internet-facing devices into SOCKS proxies."

Suspected China-Nexus Actor Exploits VMware vCenter Flaw, Deploys Babuk-Derived Ransomware

The Hacker News - 17 August 2026 13:06

Cybersecurity researchers have attributed the exploitation of a newly patched security flaw in Broadcom VMware vCenter to a suspected China-nexus advanced persistent threat (APT).The attacks involve the exploitation of CVE-2026-59310 (CVSS score: 9.8), a severe directory-traversal vulnerability in the VMware vCenter server that could be weaponized by a malicious actor to execute arbitrary code

'Turf War' Between Claude Agents Leads to Self-Replicating Malware

Dark Reading - 17 August 2026 20:26

Three testing models with the same goal but different directives engaged in "increasingly aggressive" territorial attacks on one another, according to Anthropic.

Linux Botnet Evooo1Bot Expands Mirai Capabilities Well Beyond DDoS

Dark Reading - 17 August 2026 15:44

The botnet adds exploitation modules, credential theft, and reverse SOCKS relays to turn compromised devices into persistent attacker infrastructure.