Scottish Cyber Coordination Centre

Daily Threat Bulletin

29 April 2026

Vulnerabilities

Hackers are exploiting a critical LiteLLM pre-auth SQLi flaw

BleepingComputer - 28 April 2026 18:07

Hackers are targeting sensitive information stored in the LiteLLM open-source large-language model (LLM) gateway by exploiting a critical vulnerability tracked as CVE-2026-42208.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.
CVE-2024-1708 ConnectWise ScreenConnect Path Traversal Vulnerability
CVE-2026-32202 Microsoft Windows Protection Mechanism Failure Vulnerability

Microsoft Confirms Active Exploitation of Windows Shell CVE-2026-32202

The Hacker News - 28 April 2026 12:20

Microsoft on Monday revised its advisory for a now-patched, high-severity security flaw impacting Windows Shell to acknowledge that it has been actively exploited in the wild.

Researchers Discover Critical GitHub CVE-2026-3854 RCE Flaw Exploitable via Single Git Push

The Hacker News - 29 April 2026 00:49

Cybersecurity researchers have disclosed details of a critical security vulnerability impacting GitHub.com and GitHub Enterprise Server that could allow an authenticated user to obtain remote code execution with a single “git push” command.

Microsoft fixes Entra ID flaw enabling privilege escalation

Security Affairs - 28 April 2026 12:19

Microsoft fixed a Microsoft Entra ID flaw where the Agent ID Administrator role could enable privilege escalation and account takeover. Microsoft addressed a flaw in Microsoft Entra ID that could let attackers take over service accounts.

Scottish Cyber Coordination Centre

Robinhood Vulnerability Exploited for Phishing Attacks

SecurityWeek - 28 April 2026 15:49

Legitimate-looking emails coming from Robinhood systems lured recipients to phishing websites.

Threat actors and malware

Broken VECT 2.0 ransomware acts as a data wiper for large files

BleepingComputer - 28 April 2026 18:25

Researchers are warning that the VECT 2.0 ransomware has a problem in the way it handles encryption nonces that leads to permanently destroying larger files rather than encrypt them.

Feuding Ransomware Groups Leak Each Other's Data

darkreading - 28 April 2026 21:13

When 0APT and KryBit attacked each other, they exposed infrastructure and operational data, giving defenders rare insight into ransomware operations.