Scottish Cyber Coordination Centre

Daily Threat Bulletin

8 April 2026

Vulnerabilities

Flowise AI Agent Builder Under Active CVSS 10.0 RCE Exploitation; 12,000+ Instances Exposed

The Hacker News - 07 April 2026 12:26

Threat actors are exploiting a maximum-severity security flaw in Flowise, an open-source artificial intelligence (AI) platform, according to new findings from VulnCheck. The vulnerability in question is CVE-2025-59528 (CVSS score: 10.0), a code injection vulnerability that could result in remote code execution.

Docker CVE-2026-34040 Lets Attackers Bypass Authorization and Gain Host Access

The Hacker News - 07 April 2026 21:45

A high-severity security vulnerability has been disclosed in Docker Engine that could permit an attacker to bypass authorization plugins (AuthZ) under specific circumstances. The vulnerability, tracked as CVE-2026-34040 (CVSS score: 8.8), stems from an incomplete fix for CVE-2024-41110, a maximum-severity vulnerability in the same component that came to light in July 2024.

Experts published unpatched Windows zero-day BlueHammer

Security Affairs - 07 April 2026 09:09

A disgruntled researcher released the BlueHammer Windows zero-day, a privilege escalation flaw that allows attackers to gain SYSTEM or admin rights.

Hackers exploit critical flaw in Ninja Forms WordPress plugin

BleepingComputer - 07 April 2026 19:03

A critical vulnerability in the Ninja Forms File Uploads premium add-on for WordPress allows uploading arbitrary files without authentication, which can lead to remote code execution.

Threat actors and malware

Snowflake customers hit in data theft attacks after SaaS integrator breach

BleepingComputer - 07 April 2026 16:39

Over a dozen companies have suffered data theft attacks after a SaaS integration provider was breached and authentication tokens stolen.

Scottish Cyber Coordination Centre

Fast-moving Storm-1175 uses new exploits to breach networks and drop Medusa

Security Affairs - 07 April 2026 14:20

China-based actor Storm-1175 carries out fast, financially driven ransomware attacks by exploiting newly disclosed vulnerabilities before organizations patch them. The group targets exposed systems and quickly moves from initial access to data theft and Medusa ransomware deployment.

Russia's Fancy Bear still attacking routers to boost fake sites, NCSC warns

The Register - 07 April 2026 18:02

The UK's National Cyber Security Centre (NCSC) has issued a fresh warning about Russia's ongoing targeting of routers to steal passwords and other secrets.

UK incidents

Cyberattack hits Northern Ireland's centralized school network, disrupting access for thousands

The Record from Recorded Future News - 07 April 2026 13:04

A cyberattack on a centralized school IT network in Northern Ireland has disrupted access to educational systems for hundreds of thousands of students, with authorities still working to fully restore services and determine whether any personal data was compromised.