Scottish Cyber Coordination Centre

Daily Threat Bulletin

12 May 2026

Vulnerabilities

10 questions to ask when using AI models to find vulnerabilities

NCSC - 11 May 2026 13:00

Using Artificial Intelligence to find vulnerabilities can bring added security considerations.

Instructure confirms hackers used Canvas flaw to deface portals

BleepingComputer - 11 May 2026 12:26

Education technology giant Instructure has confirmed that a security vulnerability allowed hackers to modify Canvas login portals and leave an extortion message. [...]

Google: Hackers used AI to develop zero-day exploit for web admin tool

BleepingComputer - 11 May 2026 10:02

Researchers at Google Threat Intelligence Group (GTIG) say that a zero-day exploit targeting a popular open-source web administration tool was likely generated using AI. [...]

U.S. CISA adds a flaw in BerriAI LiteLLM to its Known Exploited Vulnerabilities catalog

Security Affairs - 11 May 2026 10:14

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds a flaw in BerriAI LiteLLM to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a flaw in BerriAI LiteLLM, tracked as CVE-2026-42208 (CVSS score of 9.3), to its Known Exploited Vulnerabilities (KEV) catalog.

cPanel CVE-2026-41940 Under Active Exploitation to Deploy Filemanager Backdoor

The Hacker News - 12 May 2026 00:24

A threat actor named Mr_Rot13 has been attributed to the exploitation of a recently disclosed critical cPanel flaw to deploy a backdoor codenamed Filemanager on compromised environments.The attack exploits CVE-2026-41940, a vulnerability impacting cPanel and WebHost Manager (WHM) that could result in an authentication bypass and allow remote attackers to gain elevated control of the control.

Hackers Used AI to Develop First Known Zero-Day 2FA Bypass for Mass Exploitation

The Hacker News - 11 May 2026 22:15

Google on Monday disclosed that it identified an unknown threat actor using a zero-day exploit that it said was likely developed with an artificial intelligence (AI) system, marking the first time the technology has been put to use in the wild in a malicious context for vulnerability discovery and exploit generation.

Scottish Cyber Coordination Centre

Threat actors and malware

TeamPCP Compromises Checkmarx Jenkins AST Plugin Weeks After KICS Supply Chain Attack

The Hacker News - 12 May 2026 01:00

Checkmarx has confirmed that a modified version of the Jenkins AST plugin was published to the Jenkins Marketplace."If you are using Checkmarx Jenkins AST plugin, you need to ensure that you are using the version 2.0.13-829.vc72453fa_1c16 that was published on December 17, 2025 or previously," the cybersecurity company said in a statement over the weekend.As of writing, Checkmarx has released

Canvas System Is Online After a Cyberattack Disrupted Thousands of Schools

SecurityWeek - 11 May 2026 09:35

Tens of thousands of students studying for final exams around the world have regained access to a key online learning system after a cyberattack had earlier knocked it offline.