Scottish Cyber Coordination Centre

Daily Threat Bulletin

24 October 2025

Vulnerabilities

Critical Lanscope Endpoint Manager Bug Exploited in Ongoing Cyberattacks, CISA Confirms

The Hacker News - 23 October 2025 12:07

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Wednesday added a critical security flaw impacting Motex Lanscope Endpoint Manager to its Known Exploited Vulnerabilities (KEV) catalog, stating it has been actively exploited in the wild.

Over 250 attacks hit Adobe Commerce and Magento via critical CVE-2025-54236 flaw

Security Affairs - 23 October 2025 10:22

E-commerce security company Sansec researchers warn that threat actors are exploiting a critical flaw in Adobe Commerce and Magento, tracked as CVE-2025-54236 (CVSS 9.1), to hijack customer accounts via the REST API.

BIND Updates Address High-Severity Cache Poisoning Flaws

SecurityWeek - 23 October 2025 11:10

The vulnerabilities allow attackers to predict source ports and query IDs BIND will use, and to inject forged records into the cache.

Threat actors and malware

Russian Government Now Actively Managing Cybercrime Groups: Security Firm

SecurityWeek - 23 October 2025 15:46

The relationship between the Russian government and cybercriminal groups has evolved from passive tolerance.

North Korean Lazarus hackers targeted European defense companies

BleepingComputer - 23 October 2025 09:38

North Korean Lazarus hackers compromised three European companies in the defense sector through a coordinated Operation DreamJob campaign leveraging fake recruitment lures.

Scottish Cyber Coordination Centre

"Jingle Thief" Hackers Exploit Cloud Infrastructure to Steal Millions in Gift Cards

The Hacker News - 23 October 2025 14:22

Cybersecurity researchers have shed light on a cybercriminal group called Jingle Thief that has been observed targeting cloud environments associated with organizations in the retail and consumer services sectors for gift card fraud.

Microsoft disables File Explorer preview for downloads to block attacks

BleepingComputer - 23 October 2025 12:57

Microsoft says that the File Explorer (formerly Windows Explorer) now automatically blocks previews for files downloaded from the Internet to block credential theft attacks via malicious documents.