Scottish Cyber Coordination Centre

Daily Threat Bulletin

8 May 2025

Vulnerabilities

Cisco Patches CVE-2025-20188 (10.0 CVSS) in IOS XE That Enables Root Exploits via JWT

The Hacker News - 08 May 2025 11:27

Cisco has released software fixes to address a maximum-severity security flaw in its IOS XE Wireless Controller that could enable an unauthenticated, remote attacker to upload arbitrary files to a susceptible system.

Hackers exploit OttoKit WordPress plugin flaw to add admin accounts

BleepingComputer - 07 May 2025 12:37

Hackers are exploiting a critical unauthenticated privilege escalation vulnerability in the OttoKit WordPress plugin to create rogue admin accounts on targeted sites.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2024-6047 - GeoVision Devices OS Command Injection Vulnerability and CVE-2024-11120 - GeoVision Devices OS Command Injection Vulnerability.

Canary Exploit tool allows to find servers affected by Apache Parquet flaw

Security Affairs - 07 May 2025 15:08

A working proof-of-concept exploit for the critical Apache Parquet vulnerability CVE-2025-30065 has been released by F5 Labs, allowing the identification of vulnerable servers.

SysAid Patches 4 Critical Flaws Enabling Pre-Auth RCE in On-Premise Version

The Hacker News - 07 May 2025 18:01

Cybersecurity researchers have disclosed multiple security flaw in the on-premise version of SysAid IT support software that could be exploited to achieve pre-authenticated remote code execution with elevated privileges.

Scottish Cyber Coordination Centre

Threat actors and malware

Play ransomware affiliate leveraged zero-day to deploy malware

Security Affairs - 07 May 2025 19:43

The Play ransomware gang has exploited a Windows Common Log File System flaw, tracked as CVE-2025-29824, in zero-day attacks to gain SYSTEM privileges and deploy malware on compromised systems.

LockBit ransomware gang hacked, victim negotiations exposed

BleepingComputer - 07 May 2025 21:06

The LockBit ransomware gang has suffered a data breach after its dark web affiliate panels were defaced and replaced with a message linking to a MySQL database dump.

Researchers Uncover Malware in Fake Discord PyPI Package Downloaded 11,500+ Times

The Hacker News - 07 May 2025 14:07

Cybersecurity researchers have discovered a malicious package on the Python Package Index (PyPI) repository that masquerades as a seemingly harmless Discord-related utility but incorporates a remote access trojan.

UK Related

"Nationally Significant" Cyber-Attacks Have Doubled, UK's NCSC Reports

Infosecurity Magazine - 07 May 2025 16:15

NCSC CEO Richard Horne said the cyber agency has managed twice as many nationally significant cyber incidents in the period from September 2024 to May 2025

UK spies see 'direct connection' between Russian cyberattacks and sabotage plots

The Record from Recorded Future News - 07 May 2025 16:40

Britain's intelligence services are seeing a "direct connection between Russian cyber attacks and physical threats to our security," the country's cyber chief announced

UK Government Warns Retail Attacks Must Serve as a "Wake-up Call"

Infosecurity Magazine - 07 May 2025 11:30

Chancellor of the Duchy of Lancaster Pat McFadden said that the recent incidents impacting household names like Marks & Spencer (M&S), the Co-op and Harrods, demonstrated that cybersecurity is not a luxury but an absolute necessity.