Scottish Cyber Coordination Centre

Daily Threat Bulletin

7 May 2025

Vulnerabilities

Samsung MagicINFO 9 Server RCE flaw now exploited in attacks

BleepingComputer - 06 May 2025 14:10

Hackers are exploiting an unauthenticated remote code execution (RCE) vulnerability in the Samsung MagicINFO 9 Server to hijack devices and deploy malware.

Update ASAP: Google Fixes Android Flaw (CVE-2025-27363) Exploited by Attackers

The Hacker News - 06 May 2025 12:16

Google has released its monthly security updates for Android with fixes for 46 security flaws, including one vulnerability that it said has been exploited in the wild. The vulnerability in question is CVE-2025-27363 (CVSS score: 8.1), a high-severity flaw in the System component that could lead to local code execution without requiring any additional execution privileges.

Experts warn of a second wave of attacks targeting SAP NetWeaver bug CVE-2025-31324

Security Affairs - 06 May 2025 14:55

Threat actors launch second wave of attacks on SAP NetWeaver, exploiting webshells from a recent zero-day vulnerability. In April, ReliaQuest researchers warned that a zero-day vulnerability, tracked as CVE-2025-31324 (CVSS score of 10/10), in SAP NetWeaver is potentially being exploited. Thousands of internet-facing applications are potentially at risk.

Critical Vulnerability in AI Builder Langflow Under Attack

SecurityWeek - 06 May 2025 12:21

CISA warns organizations that threat actors are exploiting a critical-severity vulnerability in low-code AI builder Langflow.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2025-27363 - FreeType Out-of-Bounds Write Vulnerability.

Apache Parquet exploit tool detect servers vulnerable to critical flaw

BleepingComputer - 06 May 2025 15:16

A proof-of-concept exploit tool has been publicly released for a maximum severity Apache Parquet vulnerability, tracked as CVE-2025-30065, making it easy to find vulnerable servers.

Scottish Cyber Coordination Centre

Threat actors and malware

Darcula Phishing as a Service Operation Snares 800,000+ Victims

Infosecurity Magazine - 06 May 2025 11:30

Prolific PhaaS operation Darcula uses Magic Cat software to steal over 800,000 cards in a seven-month period

Third Parties and Machine Credentials: The Silent Drivers Behind 2025's Worst Breaches

The Hacker News - 06 May 2025 17:55

It wasn't ransomware headlines or zero-day exploits that stood out most in this year's Verizon 2025 Data Breach Investigations Report (DBIR) — it was what fueled them. Quietly, yet consistently, two underlying factors played a role in some of the worst breaches: third-party exposure and machine credential abuse.

Inside DragonForce, the Group Tied to M&S, Co-op and Harrods Hacks

Infosecurity Magazine - 06 May 2025 13:25

Anonymous individuals identifying as members of the DragonForce cybercriminal syndicate have claimed to be behind the cyber-attacks on Marks & Spencer, Co-op and Harrods.

UK incidents

UK Legal Aid Agency investigates cybersecurity incident

BleepingComputer - 06 May 2025 13:20

The Legal Aid Agency (LAA), an executive agency of the UK's Ministry of Justice that oversees billions in legal funding, warned law firms of a security incident and said the attackers might have accessed financial information.

UK's NCSC Offers Security Tips as Co-op Confirms Data Loss

Infosecurity Magazine - 06 May 2025 10:20

The National Cyber Security Centre has published advice for retailers while the Co-op admits customer data was stolen.