Scottish Cyber Coordination Centre

Daily Threat Bulletin

23 May 2025

Vulnerabilities

Ivanti EPMM flaw exploited by Chinese hackers to breach govt agencies

BleepingComputer - 22 May 2025 11:23

Chinese hackers have been exploiting a remote code execution flaw in Ivanti Endpoint Manager Mobile (EPMM) to breach high-profile organizations worldwide.

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-2025-4632 Samsung MagicINFO 9 Server Path Traversal Vulnerability

Critical Windows Server 2025 dMSA Vulnerability Enables Active Directory Compromise

The Hacker News - 22 May 2025 19:05

A privilege escalation flaw has been demonstrated in Windows Server 2025 that makes it possible for attackers to compromise any user in Active Directory (AD).

Critical Versa Concerto Flaws Let Attackers Escape Docker and Compromise Hosts

The Hacker News - 22 May 2025 17:36

Cybersecurity researchers have uncovered multiple critical security vulnerabilities impacting the Versa Concerto network security and SD-WAN orchestration platform that could be exploited to take control of susceptible instances.

Cisco Patches High-Severity DoS, Privilege Escalation Vulnerabilities

SecurityWeek - 22 May 2025 09:39

Cisco published 10 security advisories detailing over a dozen vulnerabilities, including two high-severity flaws in its Identity Services Engine (ISE) and Unified Intelligence Center.

Scottish Cyber Coordination Centre

Threat actors and malware

CISA: Russia's Fancy Bear Targeting Logistics, IT Firms

darkreading - 22 May 2025 18:14

Fancy Bear (APT28), a state-backed hacking group tied to Russia's Main Intelligence Directorate (GRU), is ramping up attacks on logistics and IT firms, especially those aiding Ukraine, as part of a broader cyber-espionage campaign.

FBI and Europol Disrupt Lumma Stealer Malware Network Linked to 10 Million Infections

The Hacker News - 22 May 2025 14:54

A sprawling operation undertaken by global law enforcement agencies and a consortium of private sector firms has disrupted the online infrastructure associated with a commodity information stealer known as Lumma (aka LummaC or LummaC2), seizing 2,300 domains that acted as the command-and-control (C2) backbone to commandeer infected Windows systems.

Blurring Lines Between Scattered Spider & Russian Cybercrime

darkreading - 22 May 2025 16:56

The loosely affiliated hacking group has shifted closer to ransomware gangs, raising questions about Scattered Spider's ties to the Russian cybercrime underground.

Russian hacker group Killnet returns with new identity

The Record from Recorded Future News - 22 May 2025 17:22

The Russian hacker group Killnet, once known for its noisy pro-Kremlin cyberattacks, has reappeared after months of silence — but not as the group it once was.

UK incidents

Scottish council admits ransomware crooks stole school data

The Register - 22 May 2025 10:47

Scotland's West Lothian Council has confirmed that data was stolen from its education network after the Interlock ransomware group claimed responsibility for the intrusion earlier this month.