Scottish Cyber Coordination Centre

Daily Threat Bulletin

10 October 2025

Vulnerabilities

CVE-2025-5947: WordPress Plugin flaw lets hackers access Admin accounts

Security Affairs - 09 October 2025 15:27

Threat actors are exploiting a critical vulnerability, tracked as CVE-2025-5947 (CVSS score 9.8), in the Service Finder WordPress theme's Bookings plugin.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.
CVE-2021-43798 Grafana Path Traversal Vulnerability

Threat actors and malware

Hackers Access SonicWall Cloud Firewall Backups, Spark Urgent Security Checks

The Hacker News - 09 October 2025 20:18

SonicWall on Wednesday disclosed that an unauthorized party accessed firewall configuration backup files for all customers who have used the cloud backup service.

RondoDox botnet targets 56 n-day flaws in worldwide attacks

BleepingComputer - 09 October 2025 14:17

A new large-scale botnet called RondoDox is targeting 56 vulnerabilities in more than 30 distinct devices, including flaws first disclosed during Pwn2Own hacking competitions.

Hackers now use Velociraptor DFIR tool in ransomware attacks

BleepingComputer - 09 October 2025 16:31

Threat actors have started to use the Velociraptor digital forensics and incident response (DFIR) tool in attacks that deploy LockBit and Babuk ransomware.

GitHub Copilot 'CamoLeak' AI Attack Exfiltrates Data

darkreading - 09 October 2025 20:56

While GitHub has advanced protections for its built-in AI agent, a researcher came up with a creative proof-of-concept (PoC) attack for exfiltrating code and secrets via Copilot.

Scottish Cyber Coordination Centre

Chaos Ransomware Upgrades With Aggressive New C++ Variant

darkreading - 09 October 2025 10:44

New encryption, wiper, and cryptocurrency-stealing capabilities make the evolving ransomware-as-a-service operation more dangerous than ever.

UK Related

NCSC: Observability and Threat Hunting Must Improve

Infosecurity Magazine - 09 October 2025 09:45

The UK's National Cyber Security Centre has released new guidance to help firms improve observability and threat hunting.