Scottish Cyber Coordination Centre

Daily Threat Bulletin

22 August 2025

Vulnerabilities

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-2025-43300 Apple iOS, iPadOS, and macOS Out-of-Bounds Write Vulnerability

Pre-Auth Exploit Chains Found in Commvault Could Enable Remote Code Execution Attacks

The Hacker News - 21 August 2025 23:08

Commvault has released updates to address four security gaps that could be exploited to achieve remote code execution on susceptible instances.

Microsoft reportedly cuts China's early access to bug disclosures, PoC exploit code

The Register - 21 August 2025 23:58

Microsoft has reportedly stopped giving Chinese companies proof-of-concept exploit code for soon-to-be-disclosed vulnerabilities following last month's SharePoint zero-day attacks, which appear to be related to a leak in Redmond's early-bug-notification program.

Threat actors and malware

FBI: Russia-linked group Static Tundra exploit old Cisco flaw for espionage

Security Affairs - 21 August 2025 08:51

The FBI warns that Russia-linked threat actor Static Tundra exploits Simple Network Management Protocol (SNMP) and end-of-life networking devices running an unpatched vulnerability (CVE-2018-0171) in Cisco Smart Install (SMI).

Cybercriminals Deploy CORNFLAKE.V3 Backdoor via ClickFix Tactic and Fake CAPTCHA Pages

The Hacker News - 21 August 2025 22:55

Threat actors have been observed leveraging the deceptive social engineering tactic known as ClickFix to deploy a versatile backdoor codenamed CORNFLAKE.V3. Google-owned Mandiant described the activity, which it tracks as UNC5518, as part of an access-as-a-service scheme that employs fake CAPTCHA pages as lures to trick users into providing initial access to their systems.

Scottish Cyber Coordination Centre

Hackers deploy DripDropper via Apache ActiveMQ flaw, patch systems to evade detection

Security Affairs - 21 August 2025 17:30

Red Canary researchers observed attackers exploit a 2-year-old Apache ActiveMQ vulnerability, tracked as CVE-2023-46604 (CVSS score of 10.0), to gain persistence on cloud Linux systems and deploy DripDropper malware. Uniquely, they patch the flaw post-exploit.

Hackers Using New QuirkyLoader Malware to Spread Agent Tesla, AsyncRAT and Snake Keylogger

The Hacker News - 21 August 2025 17:11

Cybersecurity researchers have disclosed details of a new malware loader called QuirkyLoader that's being used to deliver via email spam campaigns, an array of next-stage payloads ranging from information stealers to remote access trojans since November 2024.

Hackers Abuse VPS Infrastructure for Stealth, Speed

darkreading - 21 August 2025 18:42

New research highlights how threat actors abuse legitimate virtual private server offerings in order to spin up infrastructure cheaply, quietly, and fast.

Easy ChatGPT Downgrade Attack Undermines GPT-5 Security

darkreading - 21 August 2025 21:35

By using brief, plain clues in their prompts that are likely to influence the app to query older models, a user can downgrade ChatGPT for malicious ends.

UK incidents

Colt confirms customer data stolen as Warlock ransomware auctions files

BleepingComputer - 21 August 2025 17:41

UK-based telecommunications company Colt Technology Services confirms that customer documentation was stolen as Warlock ransomware gang auctions files.