Scottish Cyber Coordination Centre

Daily Threat Bulletin

21 August 2025

Vulnerabilities

Apple Patches CVE-2025-43300 Zero-Day in iOS, iPadOS, and macOS Exploited in Targeted Attacks

The Hacker News - 21 August 2025 11:17

Apple has released security updates to address a security flaw impacting iOS, iPadOS, and macOS that it said has come under active exploitation in the wild.

Google fixed Chrome flaw found by Big Sleep AI

Security Affairs - 20 August 2025 09:39

Chrome 139 addressed a high-severity vulnerability, tracked as CVE-2025-9132, in its open source high-performance JavaScript and WebAssembly engine V8. The vulnerability is an out-of-bounds write issue in the V8 JavaScript engine.

Commvault releases patches for two nasty bug chains after exploits proven

The Register - 20 August 2025 18:03

Researchers at watchTowr just published working proof-of-concept exploits for two unauthenticated remote code execution bug chains in backup giant Commvault.

FBI, Cisco Warn of Russian Attacks on 7-Year-Old Flaw

darkreading - 20 August 2025 20:39

In the past year, "Static Tundra," aka "Energetic Bear," has breached thousands of end-of-life Cisco devices unpatched against a 2018 flaw, in a campaign targeting enterprises and critical infrastructure.

Threat actors and malware

Hackers steal Microsoft logins using legitimate ADFS redirects

BleepingComputer - 20 August 2025 12:33

Hackers are using a novel technique that combines legitimate office.com links with Active Directory Federation Services (ADFS) to redirect users to a phishing page that steals Microsoft 365 logins.

Scottish Cyber Coordination Centre

"Rapper Bot" malware seized, alleged developer identified and charged

BleepingComputer - 20 August 2025 14:40

The U.S. Department of Justice (DoJ) announced charges against the alleged developer and administrator of the "Rapper Bot" DDoS-for-hire botnet.

Major password managers can leak logins in clickjacking attacks

BleepingComputer - 20 August 2025 11:49

Six major password managers with tens of millions of users are currently vulnerable to unpatched clickjacking flaws that could allow attackers to steal account credentials, 2FA codes, and credit card details.

North Korea Uses GitHub in Diplomat Cyber Attacks as IT Worker Scheme Hits 320+ Firms

The Hacker News - 20 August 2025 15:48

North Korean threat actors have been attributed to a coordinated cyber espionage campaign targeting diplomatic missions in their southern counterpart between March and July 2025.

Hackers Weaponize QR Codes in New 'Quishing' Attacks

Infosecurity Magazine - 20 August 2025 13:45

Researchers discovered two new phishing techniques where attackers split malicious QR codes or embed them into legitimate ones.

Warlock Ransomware Hitting Victims Globally Through SharePoint ToolShell Exploit

Infosecurity Magazine - 20 August 2025 12:00

Trend Micro highlighted a sophisticated post-compromise attack chain to deploy the Warlock ransomware in unpatched SharePoint on-prem environments.

UK Related

UK Retreats on Apple Encryption Backdoor Demand Following US Pressure

Infosecurity Magazine - 20 August 2025 10:40

US director of national intelligence, Tulsi Gabbard, stated that her government persuaded the UK to withdraw its controversial demand.