Scottish Cyber Coordination Centre

Daily Threat Bulletin

17 July 2025

Vulnerabilities

CVE-2025-6554 marks the fifth actively exploited Chrome Zero-Day patched by Google in 2025

Security Affairs - 16 July 2025 11:11

Google released fixes for six Chrome flaws, including one actively exploited in the wild tracked as CVE-2025-6558 (CVSS score of 8.8). CVE-2025-6558 stems from improper validation of untrusted input in Chrome's ANGLE and GPU components.

Cisco Warns of Critical ISE Flaw Allowing Unauthenticated Attackers to Execute Root Code

The Hacker News - 17 July 2025 12:07

Cisco has disclosed a new maximum-severity security vulnerability impacting Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC) that could permit an attacker to execute arbitrary code on the underlying operating system with elevated privileges.

New Fortinet FortiWeb hacks likely linked to public RCE exploits

BleepingComputer - 16 July 2025 11:58

Multiple Fortinet FortiWeb instances recently infected with web shells are believed to have been compromised using public exploits for a recently patched remote code execution (RCE) flaw tracked as CVE-2025-25257.

Threat actors and malware

Critical Golden dMSA Attack in Windows Server 2025 Enables Cross-Domain Attacks and Persistent Access

The Hacker News - 16 July 2025 18:28

Cybersecurity researchers have disclosed what they say is a "critical design flaw" in delegated Managed Service Accounts (dMSAs) introduced in Windows Server 2025.

Hackers Leverage Microsoft Teams to Spread Matanbuchus 3.0 Malware to Targeted Firms

The Hacker News - 17 July 2025 00:18

Cybersecurity researchers have flagged a new variant of a known malware loader called Matanbuchus that packs in significant features to enhance its stealth and evade detection.

Scottish Cyber Coordination Centre

SonicWall SMA devices hacked with OVERSTEP rootkit tied to ransomware

BleepingComputer - 16 July 2025 12:33

A threat actor has been deploying a previously unseen malware called OVERSTEP that modifies the boot process of fully-patched but no longer supported SonicWall Secure Mobile Access appliances.

Operation Eastwood disrupted operations of pro-Russian hacker group NoName057(16)

Security Affairs - 16 July 2025 20:51

Between 14 and 17 July, a joint international operation, known as Eastwood and coordinated by Europol and Eurojust, targeted the cybercrime network NoName057(16).

Cloudflare says 1.1.1.1 outage not caused by attack or BGP hijack

BleepingComputer - 16 July 2025 13:49

To quash speculation of a cyberattack or BGP hijack incident causing the recent 1.1.1.1 Resolver service outage, Cloudflare explains in a post mortem that the incident was caused by an internal misconfiguration.

UK incidents

Co-op confirms data of 6.5 million members stolen in cyberattack

BleepingComputer - 16 July 2025 19:29

UK retailer Co-op has confirmed that personal data of 6.5 million members was stolen in the massive cyberattack in April that shut down systems and caused food shortages in its grocery stores.