Scottish Cyber Coordination Centre

Daily Threat Bulletin

3 June 2025

Vulnerabilities

Qualcomm fixes three Adreno GPU zero-days exploited in attacks

BleepingComputer - 02 June 2025 08:11

Qualcomm has released security patches for three zero-day vulnerabilities in the Adreno Graphics Processing Unit (GPU) driver that impact dozens of chipsets and are actively exploited in targeted attacks. [...]

Experts published a detailed analysis of Cisco IOS XE WLC flaw CVE-2025-20188

Security Affairs - 02 June 2025 07:58

Technical details about a critical Cisco IOS XE WLC flaw (CVE-2025-20188) are now public, raising the risk of a working exploit emerging soon. Details of a critical vulnerability, tracked as CVE-2025-20188, impacting Cisco IOS XE WLC are now public, raising the risk of exploitation.

New Chrome Zero-Day Actively Exploited; Google Issues Emergency Out-of-Band Patch

The Hacker News - 03 June 2025 10:52

Google on Monday released out-of-band fixes to address three security issues in its Chrome browser, including one that it said has come under active exploitation in the wild.The high-severity flaw is being tracked as CVE-2025-5419, and has been flagged as an out-of-bounds read and write vulnerability in the V8 JavaScript and WebAssembly engine.

New Linux Vulnerabilities Expose Password Hashes via Core Dumps

Infosecurity Magazine - 02 June 2025 16:00

Two local information disclosure flaws in Linux crash-reporting tools have been identified exposing system data to attackers

CISA Adds Five Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA added five new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2021-32030 ASUS Routers Improper Authentication Vulnerability; CVE-2023-39780 ASUS RT-AX55 Routers OS Command Injection Vulnerability; CVE-2024-56145 Craft CMS Code Injection Vulnerability; CVE-2025-3935 ConnectWise ScreenConnect Improper Authentication Vulnerability; CVE-2025-35939 Craft CMS External Control of Assumed-Immutable Web Parameter Vulnerability.

Scottish Cyber Coordination Centre

Threat actors and malware

Microsoft and CrowdStrike partner to link hacking group names

BleepingComputer - 02 June 2025 13:56

Microsoft and CrowdStrike announced today that they've partnered to connect the aliases used for specific threat groups without actually using a single naming standard. [...]

Cryptojacking Campaign Exploits DevOps APIs Using Off-the-Shelf Tools from GitHub

The Hacker News - 02 June 2025 22:33

Cybersecurity researchers have discovered a new cryptojacking campaign that's targeting publicly accessible DevOps web servers such as those associated with Docker, Gitea, and HashiCorp Consul and Nomad to illicitly mine cryptocurrencies.Cloud security firm Wiz, which is tracking the activity under the name JINX-0132.

Sophisticated Malware Campaign Targets Windows and Linux Systems

Infosecurity Magazine - 02 June 2025 15:30

A new malware campaign targeting Windows and Linux systems has been identified, deploying tools for evasion and credential theft

Acreed Emerges as Dominant Infostealer Threat Following Lumma Takedown

Infosecurity Magazine - 02 June 2025 13:00

A report on the dark web marketplace Russian Market showed Acreed has emerged as the leading infostealer

Australia Requires Ransomware Victims to Declare Payments

Schneier on Security - 02 June 2025 12:03

A new Australian law requires larger companies to declare any ransomware payments they have made.