Scottish Cyber Coordination Centre

Daily Threat Bulletin

6 June 2025

Vulnerabilities

Critical Cisco ISE Auth Bypass Flaw Impacts Cloud Deployments on AWS, Azure, and OCI

The Hacker News - 05 June 2025 12:07

Cisco has released security patches to address a critical security flaw impacting the Identity Services Engine (ISE) that, if successfully exploited, could allow unauthenticated actors to carry out malicious actions on susceptible systems.

Hacker selling critical Roundcube webmail exploit as tech info disclosed

BleepingComputer - 05 June 2025 13:55

Hackers are actively exploiting CVE-2025-49113, a critical vulnerability in the widely used Roundcube open-source webmail application that allows remote execution.

Questions Swirl Around ConnectWise Flaw Used in Attacks

darkreading - 05 June 2025 15:48

ConnectWise issued a patch to stave off attacks on ScreenConnect customers, but the company's disclosures don't explain what the vulnerability is and when it was first exploited.

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-2025-5419 - Google Chromium V8 Out-of-Bounds Read and Write Vulnerability.

Threat actors and malware

ClickFix Attack Exploits Fake Cloudflare Turnstile to Deliver Malware

SecurityWeek - 05 June 2025 12:46

Researchers have discovered and analyzed a ClickFix attack that uses a fake Cloudflare 'humanness' check.

Scottish Cyber Coordination Centre

FBI: BADBOX 2.0 Android malware infects millions of consumer devices

BleepingComputer - 05 June 2025 18:35

The FBI is warning that the BADBOX 2.0 malware campaign has infected over 1 million home Internet-connected devices, converting consumer electronics into residential proxies that are used for malicious activity.

Backdoored Open Source Malware Repositories Target Novice Cybercriminals

SecurityWeek - 05 June 2025 14:31

A threat actor has been creating backdoored open source malware repositories to target novice cybercriminals and game cheaters.

Researchers Detail Bitter APT's Evolving Tactics as Its Geographic Scope Expands

The Hacker News - 05 June 2025 20:23

The threat actor known as Bitter has been assessed to be a state-backed hacking group that's tasked with gathering intelligence that aligns with the interests of the Indian government.

UK incidents

UK tax authority reveals scammers stole £47 million

The Record from Recorded Future News - 05 June 2025 13:59

Scammers managed to steal £47 million from the British tax authority last year after falsely claiming rebates from that were due to ordinary members of the public.