Scottish Cyber Coordination Centre

Daily Threat Bulletin

10 June 2025

Vulnerabilities

Over 84,000 Roundcube instances vulnerable to actively exploited flaw

BleepingComputer - 09 June 2025 17:14

Over 84,000 instances of the Roundcube webmail software are vulnerable to CVE-2025-49113, a critical remote code execution (RCE) vulnerability with a publicly available exploit. [...]

New Mirai botnet targets TBK DVRs by exploiting CVE-2024-3721

Security Affairs - 09 June 2025 09:54

A new variant of the Mirai botnet exploits CVE-2024-3721 to target DVR systems, using a new infection method. Researchers from Russian cybersecurity firm Kaspersky discovered a new variant of the Mirai botnet that exploits a command injection vulnerability (CVE-2024-3721) in TBK DVR-4104 and DVR-4216 digital video recording devices.

CISA Adds Erlang SSH and Roundcube Flaws to Known Exploited Vulnerabilities Catalog

The Hacker News - 10 June 2025 12:07

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added two critical security flaws impacting Erlang/Open Telecom Platform (OTP) SSH and Roundcube to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation.

Vulnerability Impacts Various Cloud Deployments of Cisco ISE

Security Magazine - 09 June 2025 09:00

A Cisco vulnerability could affect cloud deployments of Cisco Identity Services Engine (ISE) in certain systems.

Threat actors and malware

SentinelOne shares new details on China-linked breach attempt

BleepingComputer - 09 June 2025 15:26

SentinelOne has shared more details on an attempted supply chain attack by Chinese hackers through an IT services and logistics firm that manages hardware logistics for the cybersecurity firm. [...]

OpenAI bans ChatGPT accounts linked to Russian, Chinese cyber ops

Security Affairs - 09 June 2025 12:15

OpenAI banned ChatGPT accounts tied to Russian and Chinese hackers using the tool for malware, social media abuse, and U.S. satellite tech research. OpenAI banned ChatGPT accounts that were used by Russian-speaking threat actors and two Chinese nation-state actors. The blocked accounts were used to assist malware development, social media automation, and research about U.S. [...]

‘Librarian Ghouls’ Cyberattackers Strike at Night

darkreading - 09 June 2025 22:09

Since at least December, the advanced persistent threat (APT) group has been using legit tools to steal data, dodge detection, and drop cryptominers on systems belonging to organizations in Russia.

Chinese Hackers and User Lapses Turn Smartphones Into a ‘Mobile Security Crisis’

SecurityWeek - 09 June 2025 19:28

Foreign hackers have increasingly identified smartphones, other mobile devices and the apps they use as a weak link in U.S. cyberdefenses.The post Chinese Hackers and User Lapses Turn Smartphones Into a ‘Mobile Security Crisis’ appeared first on SecurityWeek.