Scottish Cyber Coordination Centre

Daily Threat Bulletin

4 July 2025

Vulnerabilities

Critical Cisco Vulnerability in Unified CM Grants Root Access via Static Credentials

The Hacker News - 03 July 2025 10:54

Cisco has released security updates to address a maximum-severity security flaw in Unified CM and Unified CM SME that could permit an attacker to login to a susceptible device as the root user, allowing them to gain elevated privileges.

Linux Users Urged to Patch Critical Sudo CVE

Infosecurity Magazine - 03 July 2025 10:00

Two elevation of privilege vulnerabilities have been discovered on the popular Sudo utility, affecting 30-50 million endpoints in the US alone.

Privilege Escalation Flaw Found in Azure Machine Learning Service

Infosecurity Magazine - 03 July 2025 16:00

A critical Azure Machine Learning flaw allows privilege escalation, risking subscription compromise.

WordPress Plugin Flaw Exposes 600,000 Sites to File Deletion

Infosecurity Magazine - 03 July 2025 16:45

A severe flaw identified in the Forminator WordPress plugin allows arbitrary file deletion and potential site takeover.

Threat actors and malware

Hunters International ransomware shuts down, releases free decryptors

BleepingComputer - 03 July 2025 07:53

The Hunters International Ransomware-as-a-Service (RaaS) operation announced today that it has officially closed down its operations and will offer free decryptors to help victims recover their data without paying a ransom.

Criminals Sending QR Codes in Phishing, Malware Campaigns

darkreading - 03 July 2025 14:23

The Anti-Phishing Working Group observed how attackers are increasingly abusing QR codes to conduct phishing attacks or to trick users into downloading malware.