Scottish Cyber Coordination Centre

Daily Threat Bulletin

1 October 2025

Vulnerabilities

Nearly 50,000 Cisco firewalls vulnerable to actively exploited flaws

BleepingComputer - 30 September 2025 13:58

Roughly 50,000 Cisco Adaptive Security Appliance (ASA) and Firewall Threat Defense (FTD) appliances exposed on the public web are vulnerable to two vulnerabilities actively leveraged by hackers.

CISA warns of critical Linux Sudo flaw exploited in attacks

BleepingComputer - 30 September 2025 10:42

Hackers are actively exploiting a critical vulnerability (CVE-2025-32463) in the sudo package that enables the execution of commands with root-level privileges on Linux operating systems.

Broadcom patches VMware Zero-Day actively exploited by UNC5174

Security Affairs - 30 September 2025 15:06

Broadcom addressed six VMware vulnerabilities, including four high-severity issues. One of these flaws has been exploited in the wild as a zero-day since mid-October 2024 by UNC5174. CVE-2025-41244 (CVSS score 7.8), allows local users to escalate to root via VMware Tools and Aria Operations.

Critical WD My Cloud bug allows remote command injection

BleepingComputer - 30 September 2025 12:07

Western Digital has released firmware updates for multiple My Cloud NAS models to patch a critical-severity vulnerability that could be exploited remotely to execute arbitrary system commands.

Researchers Disclose Google Gemini AI Flaws Allowing Prompt Injection and Cloud Exploits

The Hacker News - 30 September 2025 19:48

Cybersecurity researchers have disclosed three now-patched security vulnerabilities impacting Google's Gemini artificial intelligence (AI) assistant that, if successfully exploited, could have exposed users to major privacy risks and data theft.

Scottish Cyber Coordination Centre

Threat actors and malware

New Android RAT Klopatra Targets Financial Data

Infosecurity Magazine - 30 September 2025 16:00

New Android RAT Klopatra is targeting financial institutions using advanced evasion techniques.

New MatrixPDF toolkit turns PDFs into phishing and malware lures

BleepingComputer - 30 September 2025 15:57

A new phishing and malware distribution toolkit called MatrixPDF allows attackers to convert ordinary PDF files into interactive lures that bypass email security and redirect victims to credential theft or malware downloads.

Scattered Spider, ShinyHunters Restructure – New Attacks Underway

Security Affairs - 30 September 2025 08:20

A new report has uncovered a rapidly unfolding, and potentially much larger, global cybercrime campaign led by the notorious alliance of LAPSUS$, ShinyHunters, and Scattered Spider. Contrary to recent claims of retirement.

New China APT Strikes With Precision and Persistence

darkreading - 30 September 2025 22:09

Phantom Taurus demonstrates a deep understanding of Windows environments, including advanced components like IIServerCore, a fileless backdoor that executes in memory to evade detection.