Scottish Cyber Coordination Centre

Daily Threat Bulletin

7 November 2025

Vulnerabilities

Critical Cisco UCCX flaw lets attackers run commands as root

BleepingComputer - 06 November 2025 09:31

Cisco has released security updates to patch a critical vulnerability in the Unified Contact Center Express (UCCX) software, which could enable attackers to execute commands with root privileges.

Cisco Warns of New Firewall Attack Exploiting CVE-2025-20333 and CVE-2025-20362

The Hacker News - 06 November 2025 21:28

Cisco on Wednesday disclosed that it became aware of a new attack variant that's designed to target devices running Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software releases that are susceptible to CVE-2025-20333 and CVE-2025-20362.

Alleged Russia-linked Curly COMrades exploit Windows Hyper-V to evade EDRs

Security Affairs - 06 November 2025 10:41

Bitdefender researchers, aided by Georgia's CERT, uncovered that Curly COMrades, a group linked to Russian interests, abused Windows Hyper-V to gain covert, long-term access to victims.

JumpServer Connection Token Improper Authentication Vulnerability (CVE-2025-62712) Notice

Security Boulevard - 07 November 2025 05:02

Due to improper authentication of JumpServer's /api/v1/authentication/super-connection-token/hyper-connected endpoint, attackers with low-privilege accounts can obtain the connection tokens of all system users and connect to managed assets as them, thereby achieving unauthorized access and privilege

Multiple ChatGPT Security Bugs Allow Rampant Data Theft

darkreading - 06 November 2025 11:00

Attackers can use them to inject arbitrary prompts, exfiltrate personal user information, bypass safety mechanisms, and take other malicious actions.

Scottish Cyber Coordination Centre

Threat actors and malware

SonicWall Confirms State-Sponsored Hackers Behind September Cloud Backup Breach

The Hacker News - 06 November 2025 12:10

SonicWall has formally implicated state-sponsored threat actors as behind the September security breach that led to the unauthorized exposure of firewall configuration backup files.

ClickFix malware attacks evolve with multi-OS support, video tutorials

BleepingComputer - 06 November 2025 10:00

ClickFix attacks have evolved to feature videos that guide victims through the self-infection process, a timer to pressure targets into taking risky actions, and automatic detection of the operating system to provide the correct commands.

AI-Slop ransomware test sneaks on to VS Code marketplace

BleepingComputer - 06 November 2025 17:52

A malicious extension with basic ransomware capabilities seemingly created with the help of AI, has been published on Microsoft's official VS Code marketplace.

Clop Ransomware group claims the breach of The Washington Post

Security Affairs - 06 November 2025 23:10

The Clop Ransomware group claims the breach of The Washington Post and added the American daily newspaper to its Tor data leak site.

Android malware steals your card details and PIN to make instant ATM withdrawals

Malwarebytes - 06 November 2025 17:48

Forget card skimmers - this Android malware uses your phone's NFC to help criminals pull cash straight from ATMs.

UK incidents

Cyberattacks on UK water systems reveal rising risks to critical infrastructure

Malwarebytes - 06 November 2025 11:29

New data shows hackers targeted UK water systems five times since 2024, raising concerns about critical infrastructure defenses worldwide.