Scottish Cyber Coordination Centre

Daily Threat Bulletin

15 August 2025

Vulnerabilities

New HTTP/2 'MadeYouReset' Vulnerability Enables Large-Scale DoS Attacks

The Hacker News - 14 August 2025 21:50

Multiple HTTP/2 implementations have been found susceptible to a new attack technique called 'MadeYouReset' that could be explored to conduct powerful denial-of-service (DoS) attacks .

Microsoft fixes Windows Server bug causing cluster, VM issues

BleepingComputer - 14 August 2025 12:05

Microsoft has resolved a known issue that triggers Cluster service and VM restart issues after installing July's Windows Server 2019 security updates.

Zoom patches critical Windows flaw allowing privilege escalation

Security Affairs - 14 August 2025 09:22

Cloud-based video conferencing and online collaboration platform Zoom addressed a critical security flaw, tracked as CVE-2025-49457 (CVSS score of 9.6) in Zoom Clients for Windows. An unauthenticated user can exploit the vulnerability to conduct an escalation of privilege via network access.

Vulnerabilities in Xerox Print Orchestration Product Allow Remote Code Execution

SecurityWeek - 14 August 2025 14:47

Path traversal and XXE injection flaws allowing unauthenticated remote code execution have been patched in Xerox FreeFlow Core.

KernelSU v0.5.7 Flaw Lets Android Apps Gain Root Access

Infosecurity Magazine - 14 August 2025 16:45

A flaw in KernelSU 0.5.7 allows attackers to impersonate its manager app and gain root access to Android devices.

Scottish Cyber Coordination Centre

Threat actors and malware

Hackers Found Using CrossC2 to Expand Cobalt Strike Beacon's Reach to Linux and macOS

The Hacker News - 14 August 2025 19:46

Japan's CERT coordination center (JPCERT/CC) on Thursday revealed it observed incidents that involved the use of a command-and-control (C2) framework called CrossC2, which is designed to extend the functionality of Cobalt Strike to other platforms like Linux and Apple macOS for cross-platform system control.

Crypto24 ransomware hits large orgs with custom EDR evasion tool

BleepingComputer - 14 August 2025 14:53

The Crypto24 ransomware group has been using custom utilities to evade security solutions on breached networks, exfiltrate data, and encrypt files.

Booking.com phishing campaign uses sneaky 'ん' character to trick you

BleepingComputer - 14 August 2025 11:23

Threat actors are leveraging a Unicode character to make phishing links appear like legitimate Booking.com links in a new campaign distributing malware. The attack makes use of the Japanese hiragana character, ん, which can, on some systems, appear as a forward slash and make a phishing URL appear realistic to a person at first.