Scottish Cyber Coordination Centre

Daily Threat Bulletin

7 August 2025

Vulnerabilities

Trend Micro fixes two actively exploited Apex One RCE flaws

Security Affairs - 06 August 2025 16:34

Trend Micro released fixes for two critical vulnerabilities, tracked as CVE-2025-54948 and CVE-2025-54987 (CVSS score of 9.4), in Apex One on-prem consoles. The cybersecurity vendor confirmed that both issues were actively exploited in the wild.

ReVault flaws let hackers bypass Windows login on Dell laptops

BleepingComputer - 06 August 2025 08:58

ControlVault3 firmware vulnerabilities impacting over 100 Dell laptop models can allow attackers to bypass Windows login and install malware that persists across system reinstalls.

Researchers Uncover ECScape Flaw in Amazon ECS Enabling Cross-Task Credential Theft

The Hacker News - 07 August 2025 03:00

Cybersecurity researchers have demonstrated an “end-to-end privilege escalation chain” in Amazon Elastic Container Service (ECS) that could be exploited by an attacker to conduct lateral movement, access sensitive data, and seize control of the cloud environment.

#BHUSA: Security Researchers Uncover Critical Flaws in Axis CCTV Software

Infosecurity Magazine - 06 August 2025 22:30

Claroty researchers have uncovered four vulnerabilities in a proprietary protocol used by surveillance equipment manufacturer Axis Communications.

Threat actors and malware

Akira ransomware abuses CPU tuning tool to disable Microsoft Defender

BleepingComputer - 06 August 2025 17:15

Akira ransomware is abusing a legitimate Intel CPU tuning driver to turn off Microsoft Defender in attacks from security tools and EDRs running on target machines.

Scottish Cyber Coordination Centre

New Ghost Calls tactic abuses Zoom and Microsoft Teams for C2 operations

BleepingComputer - 06 August 2025 13:36

A new post-exploitation command-and-control (C2) evasion method called 'Ghost Calls' abuses TURN servers used by conferencing apps like Zoom and Microsoft Teams to tunnel traffic through trusted infrastructure.

CISA Releases Malware Analysis Report Associated with Microsoft SharePoint Vulnerabilities

CISA Advisories -

CISA published a Malware Analysis Report (MAR) with analysis and associated detection signatures on files related to Microsoft SharePoint vulnerabilities:
CVE-2025-49704 [CWE-94: Code Injection]
CVE-2025-49706 [CWE-287: Improper Authentication]
CVE-2025-53770 [CWE-502: Deserialization of Untrusted Data]
CVE-2025-53771 [CWE-287: Improper Authentication]
Cyber threat actors have chained CVE-2025-49704 and CVE-2025-49706 (in an exploit chain publicly known as "ToolShell") to gain unauthorized access to on-premises SharePoint servers.

#BHUSA: Malware Complexity Jumps 127% in Six Months

Infosecurity Magazine - 06 August 2025 14:00

Adversaries are prioritizing stealth over scale, according to OPSWAT's latest Threat Landscape Report.

Google suffers data breach in ongoing Salesforce data theft attacks

BleepingComputer - 06 August 2025 10:51

Google is the latest company to suffer a data breach in an ongoing wave of Salesforce CRM data theft attacks conducted by the ShinyHunters extortion group.

UK Related

NCSC Updates Cyber Assessment Framework to Build UK CNI Resilience

Infosecurity Magazine - 06 August 2025 10:45

The UK's National Cyber Security Centre has released the Cyber Assessment Framework 4.0