Scottish Cyber Coordination Centre

Daily Threat Bulletin

8 August 2025

Vulnerabilities

CISA Issues ED 25-02: Mitigate Microsoft Exchange Vulnerability

CISA Advisories -

Today, CISA issued Emergency Directive (ED) 25-02: Mitigate Microsoft Exchange Vulnerability in response to CVE-2025-53786, a vulnerability in Microsoft Exchange server hybrid deployments. ED 25-02 directs all Federal Civilian Executive Branch (FCEB) agencies with Microsoft Exchange hybrid environments to implement required mitigations by 9:00 AM EDT on Monday, August 11, 2025.

Over 100 Dell models exposed to critical ControlVault3 firmware bugs

Security Affairs - 07 August 2025 08:20

ReVault flaws in Dell ControlVault3 firmware allow firmware implants and Windows login bypass on 100+ laptop models via physical access. Cisco Talos reported five vulnerabilities collectively named ReVault (tracked as CVE-2025-24311, CVE-2025-25215, CVE-2025-24922, CVE-2025-25050, and CVE-2025-24919) in Dell's ControlVault3 firmware that expose over 100 laptop models to firmware implants and Windows login bypass.

6,500 Axis Servers Expose Remoting Protocol; 4,000 in U.S. Vulnerable to Exploits

The Hacker News - 07 August 2025 17:10

Cybersecurity researchers have disclosed multiple security flaws in video surveillance products from Axis Communications that, if successfully exploited, could expose them to takeover attacks.

SonicWall Confirms Patched Vulnerability Behind Recent VPN Attacks, Not a Zero-Day

The Hacker News - 07 August 2025 17:02

SonicWall has revealed that the recent spike in activity targeting its Gen 7 and newer firewalls with SSL VPN enabled is related to an older, now-patched bug and password reuse.

Threat actors and malware

New EDR killer tool used by eight different ransomware groups

BleepingComputer - 07 August 2025 14:58

A new Endpoint Detection and Response (EDR) killer that is considered to be the evolution of 'EDRKillShifter,' developed by RansomHub, has been observed in attacks by eight different ransomware gangs. [...]

Scottish Cyber Coordination Centre

Microsoft unveils Project Ire: AI that autonomously detects malware

Security Affairs - 07 August 2025 12:09

Microsoft's Project Ire uses AI to autonomously reverse engineer and classify software as malicious or benign. Microsoft announced Project Ire, an autonomous artificial intelligence (AI) system that can autonomously reverse engineer and classify software.

SocGholish Malware Spread via Ad Tools; Delivers Access to LockBit, Evil Corp, and Others

The Hacker News - 08 August 2025 00:56

The threat actors behind the SocGholish malware have been observed leveraging Traffic Distribution Systems (TDSs) like Parrot TDS and Keitaro TDS to filter and redirect unsuspecting users to sketchy content.

Malicious Go, npm Packages Deliver Cross-Platform Malware, Trigger Remote Data Wipes

The Hacker News - 07 August 2025 19:49

Cybersecurity researchers have discovered a set of 11 malicious Go packages that are designed to download additional payloads from remote servers and execute them on both Windows and Linux systems.

Survey: Many Organizations Hit by Ransomware Fall Victim Multiple Times

Security Boulevard - 07 August 2025 20:08

A global survey of 2,000 senior security decision-makers in organizations with between 50 and 2,000 employees finds well over a third (38%) of those who were impacted by a data breach caused by a ransomware attack were victimized multiple times in the last 12 months.

New HTTP Request Smuggling Attacks Impacted CDNs, Major Orgs, Millions of Websites

SecurityWeek - 07 August 2025 10:41

A desync attack method leveraging HTTP/1.1 vulnerabilities impacted many websites and earned researchers more than $200,000 in bug bounties.

Google Among Victims in Ongoing Salesforce Data Theft Campaign

Infosecurity Magazine - 07 August 2025 14:10

Google confirms it was among the victims of an ongoing data theft campaign targeting Salesforce instances, where publicly available business names and contact details were retrieved by the threat actor.