Scottish Cyber Coordination Centre

Daily Threat Bulletin

21 October 2025

Vulnerabilities

CISA Adds Five Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added five new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2022-48503 Apple Multiple Products Unspecified Vulnerabilit, CVE-2025-2746 Kentico Xperience Staging Sync Server Digest Password Authentication Bypass Vulnerability, CVE-2025-2747 Kentico Xperience Staging Sync Server None Password Type Authentication Bypass Vulnerability, CVE-2025-33073 Microsoft Windows SMB Client Improper Access Control Vulnerability, CVE-2025-61884 Oracle E-Business Suite Server-Side Request Forgery (SSRF) Vulnerability.

Over 75,000 WatchGuard security devices vulnerable to critical RCE

BleepingComputer - 20 October 2025 14:42

Nearly 76,000 WatchGuard Firebox network security appliances are exposed on the public web and still vulnerable to a critical issue (CVE-2025-9242) that could allow a remote attacker to execute code without authentication. [...]

ConnectWise Patches Critical Flaw in Automate RMM Tool

SecurityWeek - 20 October 2025 13:31

Attackers could exploit vulnerable deployments to intercept and tamper with communications in certain configurations.

Vulnerability in Dolby Decoder Can Allow Zero-Click Attacks

SecurityWeek - 20 October 2025 10:49

On Android, the out-of-bounds write issue can be triggered during the processing of media files without user interaction.

Threat actors and malware

Salt Typhoon Uses Citrix Flaw in Global Cyber-Attack

Infosecurity Magazine - 20 October 2025 13:15

A cyber intrusion by China-linked group Salt Typhoon has been observed targeting global infrastructure via DLL sideloading

CISA: High-severity Windows SMB flaw now exploited in attacks

BleepingComputer - 20 October 2025 14:18

CISA says threat actors are now actively exploiting a high-severity Windows SMB privilege escalation vulnerability that can let them gain SYSTEM privileges on unpatched systems. [...]

Self-spreading GlassWorm malware hits OpenVSX, VS Code registries

BleepingComputer - 20 October 2025 13:13

A new and ongoing supply-chain attack is targeting developers on the OpenVSX and Microsoft Visual Studio marketplaces with self-spreading malware called GlassWorm that has been installed an estimated 35,800 times. [...]

ColdRiver Drops Fresh Malware on Targets

darkreading - 20 October 2025 22:27

The Russia-backed threat actor's latest cyber spying campaign is a classic example of how quickly sophisticated hacking groups can pivot when exposed.

Microsoft Revokes 200+ Fake Certificates Used in Teams Malware Attack

Infosecurity Magazine - 20 October 2025 11:00

Microsoft has revoked over 200 fraudulent code-signing certificates used in a ransomware campaign involving fake Teams installers by threat group Vanilla Tempest

UK related

Russian Lynk group leaks sensitive UK MoD files, including info on eight military bases

Security Affairs - 20 October 2025 22:37

Russian hackers stole and leaked MoD files on eight RAF and Navy bases, exposing staff data in a "catastrophic" cyberattack via Dodd Group breach. Russian cybercrime group Lynx breached Dodd Group, a contractor for the UK Ministry of Defence, stealing and leaking hundreds of sensitive files on eight RAF and Royal Navy bases. The incident [...]