Scottish Cyber Coordination Centre

Daily Threat Bulletin

11 August 2026

Vulnerabilities

Multiple ClamAV Vulnerabilities Allow Remote Attacker to Trigger DoS Condition

Cyber Security News - 11 August 2026 07:02

Cisco has disclosed multiple high-severity vulnerabilities in ClamAV that could allow unauthenticated remote attackers to disrupt antivirus scanning operations and cause denial-of-service conditions.

CISA Warns of Progress LoadMaster Command Injection Vulnerability Exploited in Attacks

Cyber Security News - 10 August 2026 16:12

CISA has added a critical Progress LoadMaster vulnerability to its Known Exploited Vulnerabilities catalog after attackers were observed targeting exposed devices. Tracked as CVE-2026-8037, the flaw affects Progress LoadMaster and Progress ADC products.

CISA: SonicWall SMA1000 flaws now exploited by ransomware gangs

BleepingComputer - 10 August 2026 11:34

CISA has confirmed that ransomware gangs have begun exploiting two recently patched SonicWall SMA1000 vulnerabilities, including a maximum-severity server-side request forgery (SSRF) flaw. [...]

TrueConf Server Flaws Exploited to Replace Client Installers with PhantomCore

The Hacker News - 10 August 2026 18:03

The threat actor known as Head Mare has been observed weaponizing security flaws in unpatched TrueConf servers once again in attacks targeting Russian companies spanning instrumentation, electronics, transport, energy, IT, and software development sectors.

Coruna, DarkSword iOS Exploits Proliferate Globally

darkreading - 10 August 2026 18:09

Sophisticated iPhone exploit chains previously limited to nation-states are spreading far and wide to organized cybercrime groups.

Metabase Patches Vulnerability Exploited as Zero-Day

SecurityWeek - 10 August 2026 12:03

The security defect allows unauthenticated, remote attackers to gain administrative access to Metabase instances.

Scottish Cyber Coordination Centre

Researchers Uncover RovoBlast Vulnerability in Atlassian AI Assistant

Infosecurity Magazine - 10 August 2026 16:30

Atlassian fixed a flaw letting one crafted link make its Rovo AI assistant exfiltrate company data

Threat actors and malware

New Phishing Attack Leverage SSL/TLS Certificates to Target High-value Brands Customers Via Whatsapp

Cyber Security News - 11 August 2026 06:52

A phishing operation is using web certificates and chosen web addresses to target customers of high-value brands through WhatsApp. The activity is designed to make fraudulent pages look normal at a glance, turning a familiar security signal into part of the deception. The campaign relies on fake sites with lookalike names.

Gunra Ransomware Exploits Fortinet VPN Flaws to Bypass MFA and Steal Enterprise Data

Cyber Security News - 10 August 2026 18:24

A joint cybersecurity advisory from the FBI, CISA, the Department of Defense Cyber Crime Center, the NSA, the U.S. Secret Service, and South Korea's National Police Agency has exposed a dangerous new wave of attacks by the Gunra ransomware group, which is actively exploiting known Fortinet VPN vulnerabilities to bypass multi-factor authentication and exfiltrate sensitive

HP ThinPro TPM Disk Encryption Flaw Lets Attackers Extract LUKS Keys

Cyber Security News - 10 August 2026 17:26

A security researcher has disclosed a boot-chain weakness in HP ThinPro 8 and 9 that could allow attackers with physical access to a thin client to extract its LUKS disk-encryption key. The issue affects HP thin clients in which LUKS2 protects the operating system's encrypted root partition, and the decryption key is sealed inside the [...]

BdThemes plugins supply-chain hack creates rogue WordPress admins

BleepingComputer - 10 August 2026 18:12

A threat actor compromised the upstream infrastructure of BdThemes, a developer of premium WordPress web-design tools, and modified a remote JSON feed delivered to administrators' browsers to create rogue admin accounts. [...]

New StormEncryptor ransomware used by former Medusa affiliate

BleepingComputer - 10 August 2026 14:42

A financially motivated threat actor previously associated with the Medusa ransomware operation is now deploying a new ransomware strain called StormEncryptor. [...]

Scottish Cyber Coordination Centre

New Passkey Attacks Can Recover Synced Private Keys or Bypass Phishing-Resistant MFA

The Hacker News - 10 August 2026 18:55

Three separate research efforts last week demonstrated ways to defeat passkey protections without breaking the cryptography they rest on.Passkeys are designed to replace reusable passwords and resist phishing.

Multistate Water System Attacks Widen, Iran Suspected

darkreading - 10 August 2026 22:34

Attacks targeting water systems just keep flowing across a dozen states, against ill-secured, Internet-exposed PLCs.

OpenAI's Upcoming Astra Model Raises Autonomous Cyberattack Concerns

SecurityWeek - 10 August 2026 15:33

The current GPT-5.6-Sol has been assigned a 'high' cybersecurity threshold, but Astra could reach the maximum 'critical' threshold.

Go-Based macOS Malware Steals Crypto and Secrets

Infosecurity Magazine - 10 August 2026 11:00

A macOS malware variant has been detected stealing crypto, passwords and more

UK related

Cyber vulnerability sweep picks up Royal Navy drones sending data to China

The Register - 10 August 2026 15:25

No, no nasties to see here, guv...