Scottish Cyber Coordination Centre

Daily Threat Bulletin

5 September 2025

Vulnerabilities

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2025-38352 Linux Kernel Time-of-Check Time-of-Use (TOCTOU) Race Condition Vulnerability; CVE-2025-48543 Android Runtime Unspecified Vulnerability; CVE-2025-53690 Sitecore Multiple Products Deserialization of Untrusted Data Vulnerability.

Severe Hikvision HikCentral product flaws: What You Need to Know

Security Affairs - 04 September 2025 11:37

Hikvision HikCentral flaw allows unauthenticated users to gain admin rights, risking full control over configs, logs, and critical monitoring. Security researchers warn of three vulnerabilities impacting Hikvision HikCentral, which is a centralized management software used across many industries for video surveillance, access control, and integrated security operations.

CISA Flags TP-Link Router Flaws CVE-2023-50224 and CVE-2025-9377 as Actively Exploited

The Hacker News - 04 September 2025 16:33

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Wednesday added two security flaws impacting TP-Link wireless routers to its Known Exploited Vulnerabilities (KEV) catalog, noting that there is evidence of them being exploited in the wild.The vulnerabilities in question are listed below - CVE-2023-50224 (CVSS score: 6.5).

Two Exploited Vulnerabilities Patched in Android

SecurityWeek - 04 September 2025 08:49

Elevation of privilege flaws in Android Runtime (CVE-2025-48543) and Linux kernel (CVE-2025-38352) have been exploited in targeted attacks.

CMS Provider Sitecore Patches Exploited Critical Zero Day

Infosecurity Magazine - 04 September 2025 13:30

Google Cloud’s Mandiant successfully disrupted an active ViewState deserialization attack affecting Sitecore deployments

Threat actors and malware

Scottish Cyber Coordination Centre

Hackers exploited Sitecore zero-day flaw to deploy backdoors

BleepingComputer - 04 September 2025 15:51

Threat actors have been exploiting a zero-day vulnerability in legacy Sitecore deployments to deploy WeepSteel reconnaissance malware. [...]

Cybercriminals Exploit X's Grok AI to Bypass Ad Protections and Spread Malware to Millions

The Hacker News - 04 September 2025 16:51

Cybersecurity researchers have flagged a new technique that cybercriminals have adopted to bypass social media platform X's malvertising protections and propagate malicious links using its artificial intelligence (AI) assistant Grok.

Blast Radius of Salesloft Drift Attacks Remains Uncertain

darkreading - 04 September 2025 17:52

Many high-profile Salesloft Drift customers have disclosed data breaches as a result of a recent supply chain attack, but the extent and severity of this campaign are unclear.

GhostRedirector Emerges as New China-Aligned Threat Actor

Infosecurity Magazine - 04 September 2025 16:45

A newly identified hacking group named GhostRedirector has compromised 65 Windows servers using previously unknown tools

North Korean Hackers Exploit Threat Intel Platforms For Phishing

Infosecurity Magazine - 04 September 2025 16:00

North Korean hackers have been observed exploiting cyber threat intelligence platforms in a campaign targeting job seekers with malware-laced lures

Scattered Spider-Linked Group Claims JLR Cyber-Attack

Infosecurity Magazine - 04 September 2025 12:45

JLR said it is investigating following claims by the actor "Scattered Lapsus$ Hunters" that it had stolen data from the firm and had issued an extortion demand

Threat Actors Abuse Hexstrike-AI Tool to Accelerate Exploitation

Infosecurity Magazine - 04 September 2025 10:30

Hackers are using legitimate red team tool Hexstrike-AI to simplify and speed up vulnerability exploitation

UK related

Cyberattack on Jaguar Land Rover Disrupts Business Operations

Security Magazine - 04 September 2025 11:00

Scottish Cyber Coordination Centre

Jaguar Land Rover experienced a cyber incident that has impacted business operations.