Scottish Cyber Coordination Centre

Daily Threat Bulletin

9 December 2025

Vulnerabilities

Exploitation Activity Ramps Up Against React2Shell

darkreading - 08 December 2025 22:41

Attacks against CVE-2025-55182, which began almost immediately after public disclosure last week, have increased as more threat actors take advantage of the flaw.

U.S. CISA adds a Meta React Server Components flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 08 December 2025 10:01

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds a Meta React Server Components flaw to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a a Meta React Server Components flaw, tracked as CVE-2025-55182 (CVSS Score of 10.0), to its Known Exploited Vulnerabilities (KEV) catalog. The vulnerability is a pre-authentication remote code execution [...]

Sneeit WordPress RCE Exploited in the Wild While ICTBroadcast Bug Fuels Frost Botnet Attacks

The Hacker News - 08 December 2025 15:45

A critical security flaw in the Sneeit Framework plugin for WordPress is being actively exploited in the wild, per data from Wordfence.The remote code execution vulnerability in question is CVE-2025-6389 (CVSS score: 9.8), which affects all versions of the plugin prior to and including 8.3. It has been patched in version 8.4, released on August 5, 2025.

Critical Apache Tika Vulnerability Leads to XXE Injection

SecurityWeek - 08 December 2025 11:43

The bug allows attackers to carry out XML External Entity (XXE) injection attacks via crafted XFA files inside PDF files.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2022-37055 D-Link Routers Buffer Overflow Vulnerability, CVE-2025-66644 Array Networks ArrayOS AG OS Command Injection Vulnerability These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.

Scottish Cyber Coordination Centre

Threat actors and malware

Ransomware gangs turn to Shanya EXE packer to hide EDR killers

BleepingComputer - 08 December 2025 20:00

Several ransomware groups have been spotted using a packer-as-a-service (PaaS) platform named Shanya to assist in EDR (endpoint detection and response) killing operations. [...]

How Agentic BAS AI Turns Threat Headlines Into Defense Strategies

BleepingComputer - 08 December 2025 11:02

Picus Security explains why relying on LLM-generated attack scripts is risky and how an agentic approach maps real threat intel to safe, validated TTPs. Their breakdown shows how teams can turn headline threats into reliable defense checks without unsafe automation. [...]

Google Fortifies Chrome Agentic AI Against Indirect Prompt Injection Attacks

SecurityWeek - 08 December 2025 19:00

Chrome's new agentic browsing protections include user alignment critic, expanded origin-isolation capabilities, and user confirmations.

More than $2 billion in payments from 4,000 ransomware incidents reported to Treasury in recent years

The Record from Recorded Future News - 08 December 2025 22:15

Researchers track dozens of organizations affected by React2Shell compromises tied to China's MSS

The Record from Recorded Future News - 08 December 2025 17:30

UK related

Oracle EBS zero-day used by Clop to breach Barts Health NHS

Security Affairs - 08 December 2025 15:53

Clop ransomware stole data from Barts Health NHS after exploiting a zero-day in its Oracle E-Business Suite. Barts Health NHS confirmed that Clop ransomware group stole data by exploiting zero-day CVE-2025-61882 in its Oracle E-Business Suite. The cybercrime group added the organization to its dark web data leak site and leaked the stolen information.