Scottish Cyber Coordination Centre

Daily Threat Bulletin

4 December 2025

Vulnerabilities

Critical RSC Bugs in React and Next.js Allow Unauthenticated Remote Code Execution

The Hacker News - 04 December 2025 00:49

The vulnerability, tracked as CVE-2025-55182, carries a CVSS score of 10.0. The vulnerability has been codenamed React2shell. It allows “unauthenticated remote code execution by exploiting a flaw in how React decodes payloads sent to React.

Microsoft Silently Mitigated Exploited LNK Vulnerability

SecurityWeek - 03 December 2025 11:50

Windows now displays in the properties tab of LNK files critical information that could reveal malicious code.

Critical flaw in WordPress add-on for Elementor exploited in attacks

BleepingComputer - 03 December 2025 17:31

Attackers are exploiting a critical-severity privilege escalation vulnerability (CVE-2025-8489) in the King Addons for Elementor plugin for WordPress, which lets them obtain administrative permissions during the registration process.

Picklescan Bugs Allow Malicious PyTorch Models to Evade Scans and Execute Code

The Hacker News - 03 December 2025 16:00

Three critical security flaws have been disclosed in an open-source utility called Picklescan that could allow malicious actors to execute arbitrary code by loading untrusted PyTorch models, effectively bypassing the tool’s protections.

Chrome 143 Patches High-Severity Vulnerabilities

SecurityWeek - 03 December 2025 09:48

Chrome 143 stable was released with patches for 13 vulnerabilities, including a high-severity flaw in the V8 JavaScript engine.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.
CVE-2021-26828 OpenPLC ScadaBR Unrestricted Upload of File with Dangerous Type Vulnerability.

Threat actors and malware

Aisuru botnet behind new record-breaking 29.7 Tbps DDoS attack

BleepingComputer - 03 December 2025 10:01

In just three months, the massive Aisuru botnet launched more than 1,300 distributed denial-of-service attacks, one of them setting a new record with a peak at 29.7 terabits per second.

Deep dive into DragonForce ransomware and its Scattered Spider connection

BleepingComputer - 03 December 2025 11:05

DragonForce expanded its ransomware operation in 2025 by working with English-speaking hackers known for advanced social engineering and initial access.

Malicious Rust Crate Delivers OS-Specific Malware to Web3 Developer Systems

The Hacker News - 03 December 2025 15:09

Cybersecurity researchers have discovered a malicious Rust package that's capable of targeting Windows, macOS, and Linux systems, and features malicious functionality to stealthily execute on developer machines by masquerading as an Ethereum Virtual Machine (EVM) unit helper tool.

'ShadyPanda' Hackers Weaponize Millions of Browsers

darkreading - 03 December 2025 23:06

The China-based cyber-threat group has been quietly using malicious extensions on the Google Chrome and Microsoft Edge marketplaces to spy on millions of users.

Attackers have a new way to slip past your MFA

Malwarebytes - 03 December 2025 16:44

Attackers are using a tool called Evilginx to steal session cookies, letting them bypass the need for a multi-factor authentication (MFA) token.

UK incidents

UK's Cyber Service for Telcos Blocks 1 Billion Malicious Site Attempts

Infosecurity Magazine - 03 December 2025 17:08

A new cyber defense service has prevented almost one billion early-stage cyber-attacks in the past year, British Security Minister claims.

UK Ransomware Payment Ban to Come with Exemptions, Security Minster Say

Infosecurity Magazine - 03 December 2025 14:25

The UK government's proposed ransomware payment ban for public sector and critical infrastructure will come with national security exemptions