Scottish Cyber Coordination Centre

Daily Threat Bulletin

8 December 2025

Vulnerabilities

React2Shell flaw exploited to breach 30 orgs, 77k IP addresses vulnerable

BleepingComputer - 06 December 2025 15:07

Over 77,000 Internet-exposed IP addresses are vulnerable to the critical React2Shell remote code execution flaw (CVE-2025-55182), with researchers now confirming that attackers have already compromised over 30 organizations across multiple sectors. [...]

Researchers Uncover 30+ Flaws in AI Coding Tools Enabling Data Theft and RCE Attacks

The Hacker News - 06 December 2025 21:54

Over 30 security vulnerabilities have been disclosed in various artificial intelligence (AI)-powered Integrated Development Environments (IDEs) that combine prompt injection primitives with legitimate features to achieve data exfiltration and remote code execution.The security shortcomings have been collectively named IDEsaster by security researcher Ari Marzouk (MaccariTA).

Critical React2Shell Flaw Added to CISA KEV After Confirmed Active Exploitation

The Hacker News - 06 December 2025 18:10

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Friday formally added a critical security flaw impacting React Server Components (RSC) to its Known Exploited Vulnerabilities (KEV) catalog following reports of active exploitation in the wild.

Threat actors and malware

New wave of VPN login attempts targets Palo Alto GlobalProtect portals

BleepingComputer - 06 December 2025 11:18

A campaign has been observed targeting Palo Alto GlobalProtect portals with login attempts and launching scanning activity against SonicWall SonicOS API endpoints. [...]

Porsche outage in Russia serves as a reminder of the risks in connected vehicle security

Security Affairs - 07 December 2025 14:42

Hundreds of Porsche cars in Russia became undrivable due to a malfunction in their factory-installed satellite security system, owners say. Hundreds of Porsche cars in Russia became undrivable after their factory-installed satellite security system malfunctioned, owners and

dealers report. Drivers in several Russian cities reported sudden engine shutdowns and fuel-delivery blocks after Porsche cars lost [...]