



Daily Threat Bulletin

16 December 2025

Vulnerabilities

[Atlassian fixed maximum severity flaw CVE-2025-66516 in Apache Tika](#)

Security Affairs - 15 December 2025 16:03

Atlassian released security updates to address dozens of flaws, including multiple critical-severity vulnerabilities. Atlassian addressed dozens of vulnerabilities impacting its products, including multiple critical-severity issues.

[FreePBX Patches Critical SQLi, File-Upload, and AUTHTYPE Bypass Flaws Enabling RCE](#)

The Hacker News - 15 December 2025 21:02

Multiple security vulnerabilities have been disclosed in the open-source private branch exchange (PBX) platform FreePBX, including a critical flaw that could result in an authentication bypass under certain configurations.

[\[R1\] Nessus Versions 10.11.1 and 10.9.6 Fix Multiple Vulnerabilities](#)

Tenable Product Security Advisories - 15 December 2025 15:48

[R1] Nessus Versions 10.11.1 and 10.9.6 Fix Multiple Vulnerabilities Arnie Cabral Mon, 12/15/2025 - 09:48 Nessus leverages third-party software to help provide underlying functionality. Several of the third-party components (expat, libxml2, libxslt) were found to contain vulnerabilities, and updated versions have been made available by the providers.

[More React2Shell Exploits CVE-2025-55182, \(Mon, Dec 15th\)](#)

SANS Internet Storm Centre - 15 December 2025 14:17

Exploits for React2Shell (CVE-2025-55182) remain active.:

[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-2025-14611 Gladinet CentreStack and Triofox Hard Coded Cryptographic Vulnerability, CVE-2025-43529 Apple Multiple Products Use-After-Free WebKit Vulnerability

Threat actors and malware

[New SantaStealer malware steals data from browsers, crypto wallets](#)



Scottish
Cyber
Coordination
Centre

BleepingComputer - 15 December 2025 18:43

A new malware-as-a-service (MaaS) information stealer named SantaStealer is being advertised on Telegram and hacker forums as operating in memory to avoid file-based detection. [...]

[Google links more Chinese hacking groups to React2Shell attacks](#)

BleepingComputer - 15 December 2025 08:46

Over the weekend, Google's threat intelligence team linked five more Chinese hacking groups to attacks exploiting the maximum-severity "React2Shell" remote code execution vulnerability. [...]

[A Browser Extension Risk Guide After the ShadyPanda Campaign](#)

The Hacker News - 15 December 2025 18:25

In early December 2025, security researchers exposed a cybercrime campaign that had quietly hijacked popular Chrome and Edge browser extensions on a massive scale.

UK related

[NCSC Playbook Embeds Cyber Essentials in Supply Chains](#)

Infosecurity Magazine - 15 December 2025 11:00

The UK's National Cyber Security Centre has called on businesses to apply Cyber Essentials to suppliers

[Jaguar Land Rover confirms staff data stolen in cyberattack](#)

The Record from Recorded Future News - 15 December 2025 14:02