

Alert Bulletin

Bulletin N.: 2024-53

Publication Date: 15/10/2024

Subject: Alert 2024-53: Critical Vulnerability in Jetpack

Traffic Light Protocol (TLP): White

Description:

The WordPress Jetpack plugin has released a critical security update to address a vulnerability that allowed authenticated users to access forms submitted by other visitors.

Jetpack, developed by Automattic, is a popular plugin that enhances the functionality, security, and performance of WordPress websites. During an internal security audit, a vulnerability was discovered in Jetpack's contact form feature, affecting versions since 3.9.9 (released in 2016). This vulnerability could have allowed any logged-in user to read forms submitted by other visitors.

Although there is no evidence that this vulnerability has been exploited, the release of the update increases the risk that someone may try to take advantage of it. To mitigate the impact, Jetpack worked with the WordPress.org plugin team to release patches for all versions since 3.9.9. If you have automatic plugin updates enabled, Jetpack will update automatically, and no further action is required. However, if auto-updates are not enabled, you will need to update manually. In both cases, it is recommended to check your version to ensure the update was successful.