

Vulnerability Description:

The WP-Recall plugin for WordPress, used for registration, profiles, commerce, and more, is vulnerable to an SQL Injection attack. This problem exists in all versions and including 16.26.10. The problem is that the plugin doesn't check or protect something called "databeat". This makes it possible for hackers to use harmful code and steal private information from the website.

Severity and Metrics:

CNA: Wordfence

CVSS version v3.1

Base Score: 7.5 HIGH

Impact Score: 3.6

Exploitability Score: 3.9

Attack vector: Network

Attack Complexity: Low

privileges Required: None

User Interaction: None

Confidentiality: High

Integrity: None

Availability: None

Impact:

1. Stealing Private Information:

Hackers can take sensitive details like usernames, passwords, or other important data.

2. No Change to Data:

This issue doesn't allow data to be changed, but it can expose private information.