WP Go Maps Plugin Vulnerability Affects Up To 300K WordPress Sites via @sejournal, @martinibuster

A security advisory was published about a vulnerability affecting the WP Go Maps plugin for WordPress installed on over 300,000 websites. The flaw enables authenticated subscribers to modify map engine settings.

WP Go Maps Plugin

The WP Go Maps plugin is used by local business WordPress sites to display customizable maps on pages and posts, including contact page maps, delivery areas, and store locations. Site owners can manage map markers and map settings without writing code.

The plugin had four vulnerabilities in 2025 and seven vulnerabilities in 2024. Vulnerabilities were discovered in the previous years stretching back to 2019 but not as often.

Vulnerability

The vulnerability can be exploited by authenticated attackers with Subscriber-level access or higher. The Subscriber role is the lowest WordPress permission role. This means an attacker only needs a basic user account to exploit the issue but only if that account level is offered to users on affected websites.

The vulnerability is caused by a missing capability check in the plugin's *processBackgroundAction()* function. A capability check is used to verify whether a logged-in user is allowed to perform a specific action. Because this check is missing, the function processes requests from users who do not have permission to change plugin settings.

As a result, authenticated attackers with Subscriber-level access can modify global map engine settings used by the plugin. These settings apply site-wide and affect how the plugin functions across the website.

Wordfence described the vulnerability as an unauthorized modification of data caused by a missing capability check. In practice, this means the plugin allows low-privileged users to change global settings that should be restricted to administrators.

The Wordfence advisory explains:

> *"The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the processBackgroundAction() function in all versions up to, and including, 10.0.04. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify global map engine settings"*

Any site running an affected version of the plugin with subscriber level registration enabled is exposed to authenticated attackers.

The vulnerability affects all versions of WP Go Maps up to and including version 10.0.04. A patch is available. Site owners are recommended to update the WP Go Maps plugin to version 10.0.05 or newer to fix the vulnerability.

Featured Image by Shutterstock/Dean Drobot

https://www.searchenginejournal.com/wp-go-maps-plugin-vulnerability-affects-up-to-300k-wordpress-sites/565955/