Arbitrary Role Change/Privilege Escalation in HM Multiple Roles WordPress plugin

Updated on August 5, 2021 - Harald Eilertsen

While investigating a security advisory about an arbitrary role change/privilege escalation issue in the HM Multiple Roles WordPress plugin, the Jetpack Scan team discovered that the fix was incomplete and left the plugin still vulnerable.

The issue is fully fixed in version 1.3 of the plugin, and we advise any sites using any earlier version of this plugin to update as soon as possible.

Details

Plugin Name: HM Multiple Roles
Plugin URI: https://wordpress.org/plugins/hm-multiple-roles
Author: HM Plugin
Author URI: https://hmplugin.com/
WPScan Entry: https://wpscan.com/vulnerability/5fd2548a-08de-4417-bff1-f174dab718d5

The Vulnerability

The plugin allows a logged in administrator to assign one or more roles when creating a new user or editing an existing user. Versions before 1.1 would allow any user to assign any combination of roles themselves through the user profile page. Version 1.1 introduced a change that disables the checkboxes for selecting roles for non administrator users.

However, the fix did not check that the request was valid when submitting changes to the profile page. This allowed a low privileged user to escalate their privileges by simply enabling the check boxes for the roles they want and submitting the page.

This can be easily achieved by using the built in developer tools in the web browser as demonstrated in the video below:

Affected versions: <= 1.2
Fixed version: 1.3
CVE-ID: CVE-2021-24602
CWE: CWE-284
CWSS: 79.3

Timeline

2021-07-20: Initial notification to vendor
2021-07-27: Tried contacting vendor again through another channel
2021-07-28: Contact with vendor established
2021-08-02: Received and verified suggested fixes from vendor
2021-08-02: Fixed version released on wordpress.org

Conclusion

If you are using the HM Multiple Roles WordPress plugin version 1.2 or earlier on your site, we recommend that you upgrade to the latest version as soon as possible.

At Jetpack, we work hard to make sure your websites are protected from these types of vulnerabilities. To stay one step ahead of any new threats, check out Jetpack Scan, which includes security scanning and automated malware removal.

Credits

Original researcher: Harald Eilertsen

Thanks to the rest of the Jetpack Scan team for feedback, help, and corrections. Also thanks to the WPScan team for the prompt response to our feedback on the issue, and to HM Plugin for being responsive and promptly fixing the issue.

*This entry was posted in **Vulnerabilities**. Bookmark the **permalink**.*

Harald Eilertsen

Harald is a Certified Systems Security Professional (CISSP) with a wide background from software development and the security industry. He has a Master of Science in analog microelectronics from the Norwegian University of Science and Technology (NTNU), and has worked for companies such as Norman, Tandberg and Cisco before joining the Jetpack Scan team at Automattic.

Compare plans

Have a question?

Comments are closed for this article, but we're still here to help! Visit the support forum and we'll be happy to answer any questions.

View support forum

Search

Get news & tips from Jetpack

Enter your email address to follow this blog and receive news and updates from Jetpack!

Email Address

Subscribe

Join 111,148 other subscribers

Browse by Topic

- Affiliates (1)
- Analytics (6)
- Code snippets (32)
- Contribute (6)
- Customer Stories (6)
- Ecommerce (11)
- Events (5)
- Features (56)
- Grow (11)
- hosting (1)
- Innovate (6)
- Jetpack News (45)
- Learn (65)
- Meet Jetpack (14)
- Performance (24)
- Photos & Videos (9)
- Promotions (2)
- Releases (166)
- Search Engine Optimization (12)
- Security (75)
- Small Business (16)
- Social Media (13)
- Support Stories (3)
- Tips & Tricks (85)
- Uncategorized (5)
- Utilities & Maintenance (4)
- Vulnerabilities (18)
- Website Design (13)
- WordAds (1)
- WordCamp (3)

Jetpack Boost
Jetpack CRM
Jetpack Protect
Jetpack Search
Jetpack Social
Jetpack VideoPress
VaultPress Backup
WP Super Cache

For Agencies

Developers

Documentation
Beta Program
Contribute to Jetpack

Legal

Terms of Service
Privacy Policy
GDPR
Privacy Notice for California Users

Help

Knowledge Base
Forums
Security Library
Contact Us
Press

Social

Mobile Apps

GET IT ON Google Play
Download on the App Store