MODULE

WordPress WPLMS Theme Privilege Escalation

← BACK TO SEARCH

Disclosed
Feb 9, 2015

Created
May 30, 2018

Description

The WordPress WPLMS theme from version 1.5.2 to 1.8.4.1 allows an authenticated user of any user level to set any system option due to a lack of validation in the import_data function of /includes/func.php.

The module first changes the admin e-mail address to prevent any notifications being sent to the actual administrator during the attack, re-enables user registration in case it has been disabled and sets the default role to be administrator. This will allow for the user to create a new account with admin privileges via the default registration page found at /wp-login.php?action=register.

Authors

Evex
rastating

References

Source Code

History

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use auxiliary/admin/http/wp_wplms_privilege_escalation
msf auxiliary(wp_wplms_privilege_escalation) > show actions
    ...actions...
msf auxiliary(wp_wplms_privilege_escalation) > set ACTION < action-name >
msf auxiliary(wp_wplms_privilege_escalation) > show options
    ...show and set options...
msf auxiliary(wp_wplms_privilege_escalation) > run
```

Emergent Threat Response

Webinars & Events

Rapid7 Labs Research

Vulnerability Database

Security Fundamentals

FOR CUSTOMERS

Sign In

Support Portal

Product Documentation

Extension Library

Rapid7 Academy

Customer Escalation Portal

CONTACT SUPPORT

+1-866-390-8113

FOLLOW US

LinkedIn

X (Twitter)

Facebook

Instagram

Bluesky