MODULE

WordPress GI-Media Library Plugin Directory Traversal Vulnerability

← BACK TO SEARCH

Disclosed
N/A

Created
May 30, 2018

Description

This module exploits a directory traversal vulnerability in WordPress Plugin GI-Media Library version 2.2.2, allowing to read arbitrary files from the system with the web server privileges. This module has been tested successfully on GI-Media Library version 2.2.2 with WordPress 4.1.3 on Ubuntu 12.04 Server.

Authors

Unknown
Roberto Soares Espreto robertoespreto@gmail.com

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

RAPID7

GET STARTED

Command Platform
Exposure Management
MDR Services

TAKE ACTION

Start a Free Trial
Take a Product Tour
Get Breach Support
Contact Sales

COMPANY

About Us

Leadership

Newsroom

Our Customers

Partner Programs

Investors

Careers

STAY INFORMED

Blog

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

Accessibility Statement