

MODULE

WordPress GI-Media Library Plugin Directory Traversal Vulnerability

[TRY SURFACE COMMAND](#)[← 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

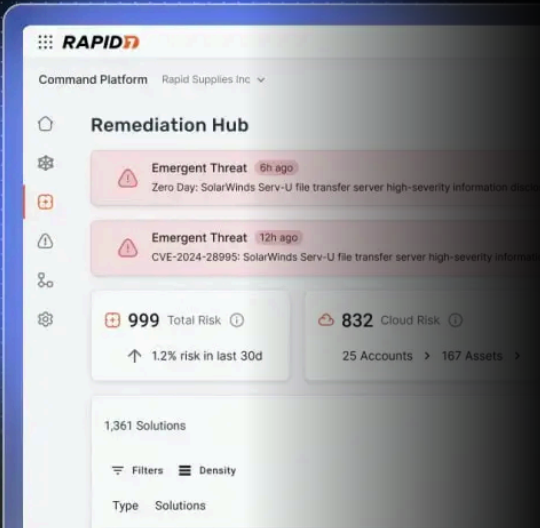
[Source Code](#)

[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
```



NEW

Explore Exposure Command

Confidently identify and prioritize exposures from endpoint to cloud with full attack surface visibility and threat-aware risk context.

[TRY IT TODAY](#)

The screenshot shows the Rapid7 Remediation Hub interface. It features a sidebar with navigation icons, a main content area with 'Remediation Hub' title, and several alert cards. Two 'Emergent Threat' alerts are visible, one from 6h ago and another from 12h ago, both related to SolarWinds Serv-U file transfer server high-severity information disclosure. Below the alerts, there are risk summary cards: '999 Total Risk' with a 12% increase in the last 30 days, and '832 Cloud Risk' associated with 25 accounts and 167 assets. At the bottom, there are filters for '1,361 Solutions' and a 'Density' view option.



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

[!\[\]\(626ce8ac21792b9405bfddfea8e0c96a_img.jpg\) LinkedIn](#)

[!\[\]\(a8f9309f944226d1420f5fed22e2b6e6_img.jpg\) X \(Twitter\)](#)

[!\[\]\(248b91fcdac4810ffd15cf33fb6aec6f_img.jpg\) Facebook](#)

[!\[\]\(899d8b7697d64725bf017d3296cfcf1b_img.jpg\) Instagram](#)

[!\[\]\(c1168d6a8b365d11e842ece304635fa7_img.jpg\) Bluesky](#)

© Rapid7

[Legal Terms](#)

[Privacy Policy](#)

[Export Notice](#)

[Trust](#)

[Cookie List](#)

[Accessibility Statement](#)