



# CVE-2015-5682

Published on: 05/22/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:16 PM UTC

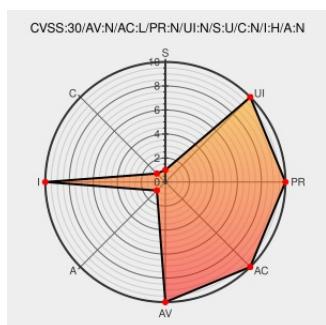
## CVE-2015-5682

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Powerplay Gallery](#) from [Powerplay Gallery Project](#) contain the following vulnerability:

upload.php in the Powerplay Gallery plugin 3.3 for WordPress allows remote attackers to create arbitrary directories via vectors related to the targetDir variable.

CVE-2015-5682 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>HIGH</b>         | <b>NONE</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>PARTIAL</b>    | <b>NONE</b>         |

## CVE References

| Description   | Tags                                                                                                                                                                                          | Link                                                      |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| Vulnerability | <a href="#">Exploit</a><br><a href="#">Third Party Advisory</a><br><a href="#">web.archive.org</a><br><a href="#">text/html</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a> | <a href="#">MISC www.vapid.dhs.org/advisory.php?v=132</a> |

oss-security - Re: Remote file upload vulnerability & SQLi in wordpress plugin wp-powerplaygallery v3.3

Exploit  
Mailing List  
www.openwall.com  
text/html

MLIST [oss-security] 20150727 Re: Remote file upload vulnerability & SQLi in wordpress plugin wp-powerplaygallery v3.3

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

### Known Affected Configurations (CPE V2.3)

| Type                                                                           | Vendor                                    | Product                           | Version | Update | Edition | Language |
|--------------------------------------------------------------------------------|-------------------------------------------|-----------------------------------|---------|--------|---------|----------|
| Application                                                                    | <a href="#">Powerplay Gallery Project</a> | <a href="#">Powerplay Gallery</a> | 3.3     | All    | All     | All      |
| Application                                                                    | <a href="#">Powerplay Gallery Project</a> | <a href="#">Powerplay Gallery</a> | 3.3     | All    | All     | All      |
| cpe:2.3:a:powerplay_gallery_project:powerplay_gallery:3.3:*:*:*:wordpress:*:*: |                                           |                                   |         |        |         |          |
| cpe:2.3:a:powerplay_gallery_project:powerplay_gallery:3.3:*:*:*:wordpress:*:*: |                                           |                                   |         |        |         |          |

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

© CVE.report 2023   |  
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)