

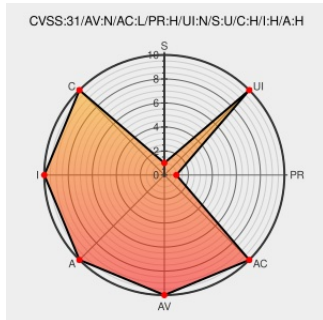


CVE-2018-6195

Published on: 01/30/2018 12:00:00 AM UTC

Last Modified on: 12/02/2022 07:09:00 PM UTC

CVE-2018-6195

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Splashing Images](#) from [Splashing Images Project](#) contain the following vulnerability:

admin/partials/wp-splashing-admin-main.php in the Splashing Images plugin (wp-splashing-images) before 2.1.1 for WordPress allows authenticated (administrator, editor, or author) remote attackers to conduct PHP Object Injection attacks via crafted serialized data in the 'session' HTTP GET parameter to wp-admin/upload.php.

CVE-2018-6195 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Full Disclosure: [CVE-2018-6194, CVE-2018-6195] PHP Object Injection + XSS in WordPress Splashing Images Plugin	Exploit Mailing List Third Party Advisory	FULLDISC 20180126 [CVE-2018-6194, CVE-2018-6195] PHP Object Injection + XSS in WordPress Splashing Images Plugin

seclists.org
text/html

WordPress Splashing Images 2.1 Cross Site Scripting /
PHP Object Injection ≈ Packet Storm

Exploit
Third Party Advisory
VDB Entry
packetstormsecurity.com
text/html

 MISC
packetstormsecurity.com/files/146109/WordPress-Splashing-Images-2.1-Cross-Site-Scripting-PHP-Object-Injection.html

Changeset 1807349 for wp-splashing-images –
WordPress Plugin Repository

Patch
Vendor Advisory
web.archive.org
text/html
Inactive Link Not Archived

 CONFIRM
plugins.trac.wordpress.org/changeset/1807349/wp-splashing-images

Splashing Images <= 2.1 - Authenticated PHP Object
Injection

Third Party Advisory
web.archive.org
text/html
Inactive Link Not Archived

 MISC wpvulndb.com/vulnerabilities/9015

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Splashing Images Project	Splashing Images	All	All	All	All
Application	Splashing Images Project	Splashing Images	All	All	All	All
cpe:2.3:a:splashing_images_project:splashing_images:*:*:*:*:wordpress:*:*:						
cpe:2.3:a:splashing_images_project:splashing_images:*:*:*:*: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](#)