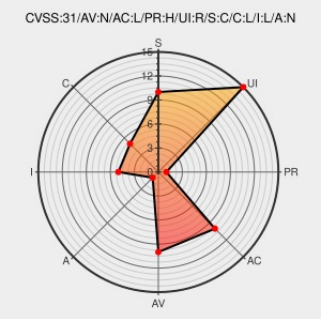
CVE-2019-16524

Published on: 09/26/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:49 PM UTC

CVE-2019-16524

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Easy Fancybox from Status301 contain the following vulnerability:

The easy-fancybox plugin before 1.8.18 for WordPress (aka Easy FancyBox) is susceptible to Stored XSS in the Settings Menu inc/class-easyfancybox.php due to improper encoding of arbitrarily submitted settings parameters. This occurs because there is no inline styles output filter.

CVE-2019-16524 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.8 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Easy FancyBox – WordPress plugin | WordPress.org	Product Third Party Advisory wordpress.org	CONFIRM wordpress.org/plugins/easy-fancybox/#developers

	text/html	
advisories/2019/SBA-ADV-20190911-01_Easy_FancyBox_WP_Plugin_Stored_XSS at public · sbaresearch/advisories · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/sbaresearch/advisories/tree/public/2019/SBA-ADV-20190911-01_Easy_FancyBox_WP_Plugin_Stored_XSS
Easy Fancybox < 1.8.18 - Authenticated Stored XSS	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC wpvulndb.com/vulnerabilities/9891

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	Status301	Easy Fancybox	All	All	All	All
Application	Status301	Easy Fancybox	All	All	All	All

cpe:2.3:a:status301:easy_fancybox:*:*:*:*:*:wordpress:*:*:

cpe:2.3:a:status301:easy_fancybox:*:*:*:*:*: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 registred 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