



CVE-2019-5983

Published on: 07/05/2019 12:00:00 AM UTC

Last Modified on: 10/07/2022 07:07:00 PM UTC

CVE-2019-5983

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

Certain versions of [Html5 Maps](#) from [Fla-shop](#) contain the following vulnerability:

Cross-site request forgery (CSRF) vulnerability in HTML5 Maps 1.6.5.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.

CVE-2019-5983 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Fla-shop.com](#) - **HTML5 Maps** version **1.6.5.6 and earlier**

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
HTML5 Maps – WordPress plugin WordPress.org	Product wordpress.org text/html	MISC wordpress.org/plugins/html5-maps/

HTML5 Maps <= 1.6.5.6 - CSRF & XSS

web.archive.org

text/html

Inactive Link

Not Archived

MISC

wpvulndb.com/vulnerabilities/9438

JVN#49575131: WordPress Plugin "HTML5 Maps" vulnerable to cross-site request forgery

Third Party Advisory

jvn.jp

text/xml

MISC

jvn.jp/en/jp/JVN49575131/index.html

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	Fla-shop	Html5 Maps	All	All	All	All
Application	Fla-shop	Html5 Maps	All	All	All	All

cpe:2.3:a:fla-shop:html5_maps:*:*:*:*:*:

cpe:2.3:a:fla-shop:html5_maps:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →