



CVE-2019-15150

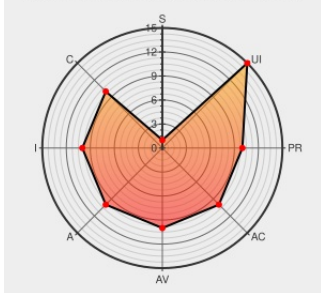
Published on: 08/18/2019 12:00:00 AM UTC

Last Modified on: 03/08/2023 01:21:00 AM UTC

CVE-2019-15150

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

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Mw-oauth2client](#) from [Schine.games](#) contain the following vulnerability:

In the OAuth2 Client extension before 0.4 for MediaWiki, a CSRF vulnerability exists due to the OAuth2 state parameter not being checked in the callback function.

CVE-2019-15150 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

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
Full Disclosure: [CVE-2019-15150] CSRF in MediaWiki extension OAuth2 Client 0.3	seclists.org text/html	FULLDISC 20190825 [CVE-2019-15150] CSRF in MediaWiki extension OAuth2 Client 0.3
Release MW OAuth2 Client 0.4	Release Notes	CONFIRM github.com/Schine/MW-OAuth2Client/releases/tag/v0.4

(Security Fix) · Schine/MW- OAuth2Client · GitHub	Third Party Advisory github.com text/html	
Bugtraq: [CVE-2019-15150] CSRF in MediaWiki extension OAuth2 Client 0.3	Mailing List Third Party Advisory seclists.org text/html	 BUGTRAQ 20190819 [CVE-2019-15150] CSRF in MediaWiki extension OAuth2 Client 0.3
oss-security - [CVE-2019-15150] CSRF in MediaWiki extension OAuth2 Client 0.3	Mailing List Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20190818 [CVE-2019-15150] CSRF in MediaWiki extension OAuth2 Client 0.3
MediaWiki OAuth2 Client 0.3 Cross Site Request Forgery ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/154140/MediaWiki-OAuth2-Client-0.3-Cross-Site-Request-Forgery.html
Enforce/verify state parameter of callback · Schine/MW- OAuth2Client@6a4fe45 · GitHub	Patch Third Party Advisory github.com text/html	 CONFIRM github.com/Schine/MW-OAuth2Client/commit/6a4fe450ddd72ad4e826d9d63b2d69512bd10d1

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	Schine.games	Mw-oauth2client	All	All	All	All
Application	Schine.games	Mw-oauth2client	All	All	All	All
cpe:2.3:a:schine.games:mw-oauth2client:*****:.*						
cpe:2.3:a:schine.games:mw-oauth2client:*****:.*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)