



CVE-2022-3119

Published on: Not Yet Published

Last Modified on: 09/28/2022 04:28:00 PM UTC

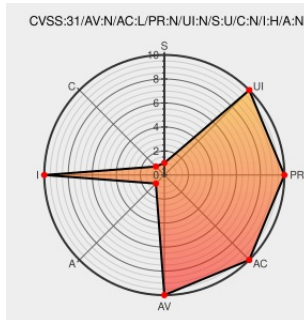
CVE-2022-3119

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [OAuth Client Single Sign On](#) from [OAuth Client Single Sign On Project](#) contain the following vulnerability:

The OAuth client Single Sign On WordPress plugin before 3.0.4 does not have authorisation and CSRF when updating its settings, which could allow unauthenticated attackers to update them and change the OAuth endpoints to ones they controls, allowing them to then be authenticated as admin if they know the correct email address

CVE-2022-3119 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Unknown - OAuth client Single Sign On for WordPress (OAuth 2.0 SSO)** version < 3.0.4

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
OAuth client Single Sign On for WordPress < 3.0.4 - Unauthenticated Settings Update to Authentication Bypass WordPress Security Vulnerability	web.archive.org text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/55b83cee-a8a5-4f9d-a976-a3eed9a558e5

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	OAuth Client Single Sign On Project	OAuth Client Single Sign On	All	All	All	All
cpe:2.3:a:oauth_client_single_sign_on_project:oauth_client_single_sign_on:*:*:*:*:wordpress:*:*:						

Discovery Credit

Lana Codes

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-3119 : The OAuth client Single Sign On WordPress plugin before 3.0.4 does not have authorisation and CSRF... twitter.com/i/web/status/1...	2022-09-26 12:44:44
 @LinInfoSec	Wordpress - CVE-2022-3119: wpscan.com/vulnerability/...	2022-09-26 16:00:34
 @phpadvisories	CVE-2022-3119 OAuth Client Single Sign On Plugin up to 3.0.3 on WordPress Setting improper authentication zpr.io/pwNCBrtWtk6H #phpsec	2022-09-26 17:24:55
 /r/netcve	CVE-2022-3119	2022-09-26 13:39:11

[← 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](#)