

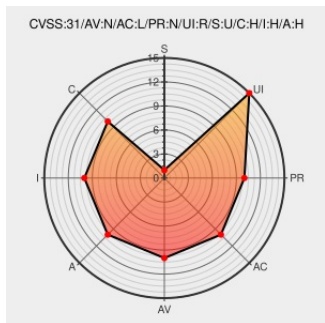


CVE-2015-9284

Published on: 04/26/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:21 PM UTC

CVE-2015-9284

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

Certain versions of [Omniauth](#) from [Omniauth](#) contain the following vulnerability:

The request phase of the OmniAuth Ruby gem (1.9.1 and earlier) is vulnerable to Cross-Site Request Forgery when used as part of the Ruby on Rails framework, allowing accounts to be connected without user intent, user interaction, or feedback to the user. This permits a secondary account to be able to sign into the web application as the

primary account.

CVE-2015-9284 has been assigned by [h](#) support@hackerone.com 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
Resolving CVE 2015 9284 · omniauth/omniauth Wiki · GitHub	Mitigation Third Party Advisory	MISC github.com/omniauth/omniauth/wiki/Resolving-

github.com
text/html

CVE-2015-9284

Protect request phase against CSRF. by DouweM · Pull Request #1 · omniauth/omniauth-rails · GitHub

Third Party Advisory
github.com
text/html

MISC github.com/omniauth/omniauth-rails/pull/1

Protect request phase against CSRF when Rails is used. by DouweM · Pull Request #809 · omniauth/omniauth · GitHub

Patch
Third Party Advisory
github.com
text/html

MISC github.com/omniauth/omniauth/pull/809

oss-security - CVE Request: CSRF vulnerability in OmniAuth request phase

Mailing List
Patch
Third Party Advisory
www.openwall.com
text/html

MLIST [oss-security] 20150526 CVE Request: CSRF vulnerability in OmniAuth request phase

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	Omniauth	Omniauth	All	All	All	All

cpe:2.3:a:omniauth:omniauth:*:*:*:*:ruby:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →