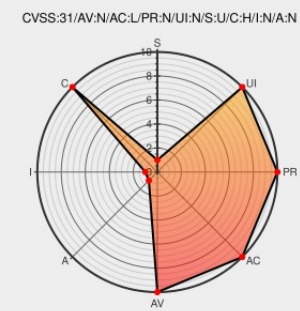
CVE-2017-18076

Published on: 01/26/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:55 PM UTC

CVE-2017-18076

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

In strategy.rb in OmniAuth before 1.3.2, the authenticity_token value is improperly protected because POST (in addition to GET) parameters are stored in the session and become available in the environment of the callback phase.

CVE-2017-18076 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

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	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
#888523 - ruby-omniauth: CVE-2017-18076: security issue in returning post	Issue Tracking, Third Party Advisory, bugs.debian.org, text/html	CONFIRM bugs.debian.org/888523

parameters from session in callback phase - Debian Bug report logs		
Debian -- Security Information -- DSA-4109-1 ruby-omniauth	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4109
security issue in returning post parameters from session in callback phase by lalithr95 · Pull Request #867 · omniauth/omniauth · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/omniauth/omniauth/pull/867
security issue in returning post parameters from session in callback phase by lalithr95 · Pull Request #867 · omniauth/omniauth · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/omniauth/omniauth/pull/867/commits/71866c5264122e196847a3980c43051446a03e9

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
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Omniauth	Omniauth	All	All	All	All
Application	Omniauth	Omniauth	All	All	All	All

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*

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

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

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