

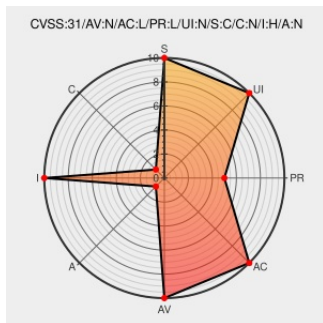


CVE-2020-26254

Published on: 12/08/2020 12:00:00 AM UTC

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

CVE-2020-26254 - advisory for GHSA-49r3-2549-3633

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

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

omniauth-apple is the OmniAuth strategy for "Sign In with Apple" (RubyGem omniauth-apple). In omniauth-apple before version 1.0.1 attackers can fake their email address during authentication. This vulnerability impacts applications using the omniauth-apple strategy of OmniAuth and using the info.email field of OmniAuth's Auth Hash

Schema for any kind of identification. The value of this field may be set to any value of the attacker's choice including email addresses of other users. Applications not using info.email for identification but are instead using the uid field are not impacted in the same manner. Note, these applications may still be negatively affected if the value of info.email is being used for other purposes. Applications using affected versions of omniauth-apple are advised to upgrade to omniauth-apple version 1.0.1 or later.

CVE-2020-26254 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [nho-soya](#) - omniauth-apple version < 1.0.1

CVSS3 Score: **7.7 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

NONE

PARTIAL

NONE

CVE References

Description	Tags	Link
omniauth-apple/CHANGELOG.md at master · nhosoya/omniauth-apple · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/nhosoya/omniauth-apple/blob/master/CHANGELOG.md#101---2020-12-03
Use only verified email address to prevent fake email address · nhosoya/omniauth-apple@b37d540 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/nhosoya/omniauth-apple/commit/b37d5409213adae2ca06a67fec14c8d3d07d9016
Vulnerability allows attacker to fake their email address during authentication · Advisory · nhosoya/omniauth-apple · GitHub	Exploit Mitigation Third Party Advisory github.com text/html	CONFIRM github.com/nhosoya/omniauth-apple/security/advisories/GHSA-49r3-2549-3633

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-apple Project	Omniauth-apple	All	All	All	All
Application	Omniauth-apple Project	Omniauth-apple	All	All	All	All

cpe:2.3:a:omniauth-apple_project:omniauth-apple:*:*:*:*:ruby:*:*:

cpe:2.3:a:omniauth-apple_project:omniauth-apple:*:*:*:*:ruby:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →