

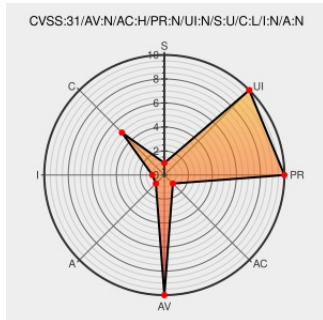


CVE-2016-5429

Published on: 09/03/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:09 PM UTC

CVE-2016-5429

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

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

jose-php before 2.2.1 does not use constant-time operations for HMAC comparison, which makes it easier for remote attackers to obtain sensitive information via a timing attack, related to JWE.php and JWS.php.

CVE-2016-5429 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **LOW** severity.

CVSS3 Score: **3.7 - LOW**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
explicit alg check & secure hash comparison · nov/jose-php@1cce55e · GitHub	Patch github.com text/html	CONFIRM github.com/nov/jose-php/commit/1cce55e27adf0274193eb1cd74b927a398a3df4b#diff-2a982d82ef0f673fd0ba2beba0e18420R138
Jose-PHP Multiple Information Disclosure	Third Party Advisory	BID 92743

Vulnerabilities

VDB Entry

cve.report (archive)

text/html

one more hash_equals, and better CEK decryption error handling · nov/jose-php@f03b986 · GitHub

Patch

github.com

text/html

CONFIRM

github.com/nov/jose-php/commit/f03b986b4439e20b0fd635109b48afe96cf0099b#diff-37b0d289d6375ba4a7740401950ccdd6R287

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	Jose-php Project	Jose-php	All	All	All	All
cpe:2.3:a:jose-php_project:jose-php:*****:*****:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→