



CVE-2016-5430

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

Last Modified on: 03/23/2021 11:27:10 PM UTC

CVE-2016-5430

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

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

The RSA 1.5 algorithm implementation in the JOSE_JWE class in JWE.php in jose-php before 2.2.1 lacks the Random Filling protection mechanism, which makes it easier for remote attackers to obtain cleartext data via a Million Message Attack (MMA).

CVE-2016-5430 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	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
Jose-PHP CVE-2016-5430 remote security Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 92741

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-37b0d289d6375ba4a7740401950ccdd6R199

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

No vendor comments have been submitted for this CVE