



CVE-2016-5431

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2016-5431
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-07 15:15:00 UTC
Updated	2023-03-03 15:53:00 UTC
Description	The PHP JOSE Library by Gree Inc. before version 2.2.1 is vulnerable to key confusion/algorithm substitution in the JWS co

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php Jose Project	Php Jose	All	All	All	All
Application	Php Jose Project	Php Jose	All	All	All	All

References

Reference	Source	Link	Tags
explicit alg check & secure hash comparison · nov/jose-php@1cce55e · GitHub	CONFIRM	github.com	Patch, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered 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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report