CVE-2017-18239

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-18239
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-18 03:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	A time-sensitive equality check on the JWT signature in the JsonWebToken.validate method in main/scala/authentikat/jwt/J

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Authentikat-jwt Project	Authentikat-jwt	All	All	All	All

References

Reference	Sour
add option to do full comparison to prevent time based guessing of the private key · Issue #12 · jasongoodwin/authentikat-jwt · GitHub	MISC
Use constant-time string comparison for sigs by anfedorov · Pull Request #36 · jasongoodwin/authentikat-jwt · GitHub	MISC
Use constant-time string comparison for sigs · jasongoodwin/authentikat-jwt@2d2fa0d · GitHub	MISC
CVE Program record	CVE.
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981339 Java (maven) Security Update for com.jason-goodwin:authentikat-jwt_2.12 (GHSA-3rhm-67j6-42jq)

Free CVE JSON API cve.report/api

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