CVE-2017-1000246

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

Summary

CVE	CVE-2017-1000246
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-17 04:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Python package pysaml2 version 4.4.0 and earlier reuses the initialization vector across encryptions in the IDP server, resu

Risk And Classification

Problem Types: CWE-330

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pysaml2 Project	Pysaml2	All	All	All	All
Application	Pysaml2 Project	Pysaml2	All	All	All	All

References

Reference	Source
Reuse of AES initialization vector in AESCipher / UsernamePasswordMako / Server · Issue #417 · IdentityPython/pysaml2 · GitHub	MISC
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981122 Python (pip) Security Update for pysaml2 (GHSA-cq94-qf6q-mf2h)

Free CVE JSON API cve.report/api

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