



# CVE-2017-1000246

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-1000246
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-11-17 04:29:00 UTC
<b>Updated</b>	2019-10-03 00:03:00 UTC
<b>Description</b>	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	<a href="#">Pysaml2 Project</a>	<a href="#">Pysaml2</a>	All	All	All	All
Application	<a href="#">Pysaml2 Project</a>	<a href="#">Pysaml2</a>	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.OF
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)

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)