



CVE-2016-10127

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2016-10127
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-03 15:59:00 UTC
Updated	2017-03-08 01:07:00 UTC
Description	PySAML2 allows remote attackers to conduct XML external entity (XXE) attacks via a crafted SAML XML request or response.

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Type
#850716 - python-pysaml2: CVE-2016-10149 - Debian Bug report logs	MISC	bugs.debian.org	Miscellaneous
python-pysaml2 CVE-2016-10127 XML External Entity Injection Vulnerability	BID	www.securityfocus.com	Vulnerability
Fix XXE in XML parsing (related to #366) · rohe/pysaml2@6e09a25 · GitHub	MISC	github.com	Patch
PySAML vulnerable to XXE · Issue #366 · rohe/pysaml2 · GitHub	MISC	github.com	Issue
oss-security - Re: CVE request: python-pysaml2 XML external entity attack	MLIST	www.openwall.com	Miscellaneous
Fix XXE in XML parsing (related to #366) by fruechel · Pull Request #379 · rohe/pysaml2 · GitHub	MISC	github.com	Issue
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)