



# CVE-2016-10149

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

## Summary

<b>CVE</b>	CVE-2016-10149
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-03-24 14:59:00 UTC
<b>Updated</b>	2018-01-05 02:30:00 UTC
<b>Description</b>	XML External Entity (XXE) vulnerability in PySAML2 4.4.0 and earlier allows remote attackers to read arbitrary files via a cr

## Risk And Classification

**Problem Types:** CWE-611

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Pysaml2 Project</a>	<a href="#">Pysaml2</a>	All	All	All	All

## References

Reference	Source	Link	T
Fix XXE in XML parsing (related to #366) · rohe/pysaml2@6e09a25 · GitHub	CONFIRM	<a href="#">github.com</a>	Is
Debian -- Security Information -- DSA-3759-1 python-pysaml2	DEBIAN	<a href="#">www.debian.org</a>	TI
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>	
PySAML vulnerable to XXE · Issue #366 · rohe/pysaml2 · GitHub	MISC	<a href="#">github.com</a>	Is
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>	
oss-security - Re: CVE request: python-pysaml2 XML external entity attack	MLIST	<a href="#">www.openwall.com</a>	M
python-pysaml2 CVE-2016-10149 XML Entity Expansion Denial of Service Vulnerability	BID	<a href="#">www.securityfocus.com</a>	
#850716 - python-pysaml2: CVE-2016-10149 - Debian Bug report logs	CONFIRM	<a href="#">bugs.debian.org</a>	Is
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>	
Fix XXE in XML parsing (related to #366) by fruechel · Pull Request #379 · rohe/pysaml2 · GitHub	CONFIRM	<a href="#">github.com</a>	Is
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	cc

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

981143 Python (pip) Security Update for pysaml2 (GHSA-c2vx-49jm-h3f6)

© [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](#)