CVE-2016-10149

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

Summary

CVE	CVE-2016-10149
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-24 14:59:00 UTC
Updated	2018-01-05 02:30:00 UTC
Description	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	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Pysaml2 Project	Pysaml2	All	All	All	All

References

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

NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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