CVE-2020-5390

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

Summary

CVE	CVE-2020-5390
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-13 19:15:00 UTC
Updated	2023-02-01 17:08:00 UTC
Description	PySAML2 before 5.0.0 does not check that the signature in a SAML document is enveloped and thus signature wrapping is

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Pysaml2 Project	Pysaml2	All	All	All	All
Application	Pysaml2 Project	Pysaml2	All	All	All	All

References

Reference	Source	Link	Tags
Fix XML Signature Wrapping (XSW) vulnerabilities · IdentityPython/pysaml2@5e9d5ac · GitHub	CONFIRM	github.com	Patch, Thir
USN-4245-1: PySAML2 vulnerability | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	
Debian -- Security Information -- DSA-4630-1 python-pysaml2	DEBIAN	www.debian.org	
Release Version 5.0.0 · IdentityPython/pysaml2 · GitHub	CONFIRM	github.com	Release No
pysaml2 · PyPI	MISC	pypi.org	Product, Th

Release version 5.0.0 · IdentityPython/pysaml2@f27c7e7 · GitHub	CONFIRM	github.com	Patch, Thir
[SECURITY] [DLA 2119-1] python-pysaml2 security update	MLIST	lists.debian.org	
Releases · IdentityPython/pysaml2 · GitHub	CONFIRM	github.com	Release No
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981492 Python (pip) Security Update for pysaml2 (GHSA-qf7v-8hj3-4xw7)