



CVE-2021-21239

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

Summary

CVE	CVE-2021-21239
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-21 15:15:00 UTC
Updated	2021-03-10 21:00:00 UTC
Description	PySAML2 is a pure python implementation of SAML Version 2 Standard. PySAML2 before 6.5.0 has an improper verificatio

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	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
pysaml2 · PyPI	MISC	pypi.org	Product, Third Party A
Unspecified xmlsec1 key-type preference · Advisory · IdentityPython/pysaml2 · GitHub	CONFIRM	github.com	Third Party A
[SECURITY] [DLA 2577-1] python-pysaml2 security update	MLIST	lists.debian.org	Mailing List, Third Party A
Release Version 6.5.0 · IdentityPython/pysaml2 · GitHub	MISC	github.com	Third Party A
Merge pull request from GHSA-5p3x-r448-pc62 · IdentityPython/pysaml2@46578df · GitHub	MISC	github.com	Patch, Third Party A
[xmlsec] Xmlsec preferring KeyValue element over explicitly loaded public keys?	MISC	www.aleksey.com	Exploit, Mailing List, Third Party A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179958 Debian Security Update for python-pysaml2 (CVE-2021-21239)

198493 Ubuntu Security Notification for PySAML2 Vulnerability (USN-5066-1)

501681 Alpine Linux Security Update for py3-saml2

501905 Alpine Linux Security Update for py3-saml2

690445 Free Berkeley Software Distribution (FreeBSD) Security Update for pysaml2 (fb67567a-5d95-11eb-a955-08002728f74c)

982936 Python (pip) Security Update for pysaml2 (GHSA-5p3x-r448-pc62)

© [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](#)