

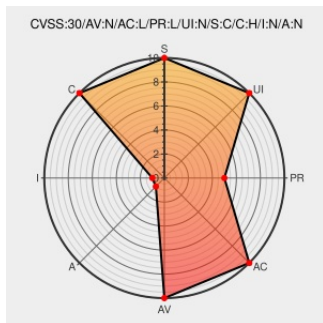


CVE-2017-11427

Published on: 04/17/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:24 PM UTC

CVE-2017-11427

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Pythonsaml](#) from [OneLogin](#) contain the following vulnerability:

OneLogin PythonSAML 2.3.0 and earlier may incorrectly utilize the results of XML DOM traversal and canonicalization APIs in such a way that an attacker may be able to manipulate the SAML data without invalidating the cryptographic signature, allowing the attack to potentially bypass authentication to SAML service providers.

CVE-2017-11427 has been assigned by security@duo.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **OneLogin** - **PythonSAML** version **2.3.0**

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Duo Finds SAML Vulnerabilities Affecting Multiple Implementations Duo	Exploit	MISC duo.com/blog/duo-finds-

Security

Technical Description

Third Party Advisory

duo.com

text/html

saml-vulnerabilities-affecting-multiple-implementations

Vulnerability Note VU#475445 - Multiple SAML libraries may allow authentication bypass via incorrect XML canonicalization and DOM traversal

Third Party Advisory

US Government Resource

www.kb.cert.org

text/html

MISC

www.kb.cert.org/vuls/id/475445

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

982987 Python (pip) Security Update for python-saml (GHSA-j8j8-348v-wfm3)

Exploit/POC from Github

The Demo for CVE-2017-11427

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Onelogin	Pythonsaml	All	All	All	All
cpe:2.3:a:onelogin:pythonsaml:*****:						

Discovery Credit

Kelby Ludwig of Duo Security

← Previous ID

Next ID →