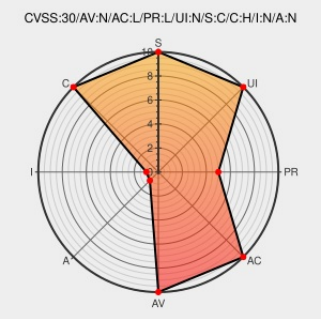
CVE-2017-11428

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

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

CVE-2017-11428

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ruby-saml from Onelogin contain the following vulnerability:

OneLogin Ruby-SAML 1.6.0 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-2017-11428 has been assigned by security@duo.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **OneLogin** - **Ruby-SAML** version **1.6.0**

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Onelogin	Ruby-saml	All	All	All	All

cpe:2.3:a:onelogin:ruby-saml:*:*:*:*:*:*:*:*:

Discovery Credit

Kelby Ludwig of Duo Security

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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.

CVE.report and Source URL Uptime Status status.cve.report