



CVE-2021-27736

Published on: 04/22/2021 12:00:00 AM UTC

Last Modified on: 04/27/2021 05:23:00 PM UTC

CVE-2021-27736

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

Certain versions of [Saml V2](#) from [Fusionauth](#) contain the following vulnerability:

FusionAuth fusionauth-samlv2 before 0.5.4 allows XXE attacks via a forged AuthnRequest or LogoutRequest because parseFromBytes uses javax.xml.parsers.DocumentBuilderFactory unsafely.

CVE-2021-27736 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
	www.compass-security.com text/plain	MISC www.compass-security.com/fileadmin/Research/Advisories/2021-03_CSNC-2021-004_FusionAuth_SAML_Library_XML_External_Entity.txt
Refactor utility methods into SAMLTools,	github.com	MISC github.com/FusionAuth/fusionauth-

add tests. · FusionAuth/fusionauth-samlv2@c66fb68 · GitHub

text/html

samlv2/commit/c66fb689d50010662f705d5b585c6388ce555dbd

Comparing 0.5.3...0.5.4 · FusionAuth/fusionauth-samlv2 · GitHub

github.com

text/html

MISC github.com/FusionAuth/fusionauth-samlv2/compare/0.5.3...0.5.4

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	Fusionauth	Saml V2	All	All	All	All
cpe:2.3:a:fusionauth:saml_v2:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← Previous ID

Next ID →