



CVE-2019-20438

Published on: 01/27/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:50 PM UTC

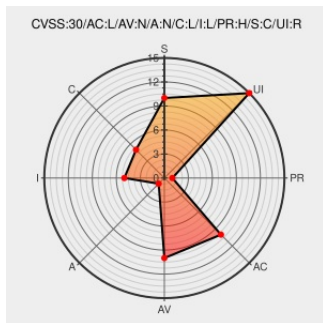
CVE-2019-20438

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Api Manager](#) from [Wso2](#) contain the following vulnerability:

An issue was discovered in WSO2 API Manager 2.6.0. A potential stored Cross-Site Scripting (XSS) vulnerability has been identified in the inline API documentation editor page of the API Publisher.

CVE-2019-20438 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.8 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

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

CVE References

Description	Tags	Link
Stored Cross Site Scripting (XSS) in 'inline API documentation editor page' WSO2 API Manager version 2.6.0 WSO2 Product · Issue #22 · cybersecurityworks/Disclosed · GitHub	Third Party Advisory github.com text/html	MISC github.com/cybersecurityworks/Disclosed/issues/22

CVE-2019-20438 - Stored Cross-Site Scripting (XSS) in WSO2

Exploit

Third Party Advisory

cybersecurityworks.com

text/html

CSW

MISC

cybersecurityworks.com/zerodays/cve-2019-20438-wso2.html

Security Advisory WSO2-2019-0645 - WSO2 Platform Security - WSO2 Documentation

Vendor Advisory

docs.wso2.com

text/html

MISC

docs.wso2.com/display/Security/Security+Advisory+WSO2-2019-0645

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	Wso2	Api Manager	2.6.0	All	All	All
Application	Wso2	Api Manager	2.6.0	All	All	All

cpe:2.3:a:wso2:api_manager:2.6.0:****:****:

cpe:2.3:a:wso2:api_manager:2.6.0:****:****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→