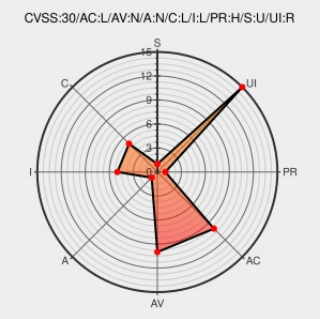
CVE-2019-20435

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

Last Modified on: 11/10/2022 04:47:00 AM UTC

CVE-2019-20435

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 reflected XSS attack could be performed in the inline API documentation editor page of the API Publisher by sending an HTTP GET request with a harmful docName request parameter.

CVE-2019-20435 has been assigned by 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
CVE-2019-20435 - Reflected Cross-Site Scripting (XSS) in WSO2 Product	cybersecurityworks.com text/html	MISC cybersecurityworks.com/zerodays/cve-2019-20435-wso2.html
Reflected Cross Site Scripting (XSS) in WSO2 Product (WSO2 API Manager version 2.6.0) · Issue	Exploit Third Party Advisory	MISC github.com/cybersecurityworks/Disclosed/issues/18

#18 · cybersecurityworks/Disclosed · GitHub	github.com text/html	
Security Advisory WSO2-2019-0633 - WSO2 Platform Security - WSO2 Documentation	Vendor Advisory docs.wso2.com text/html	MISC docs.wso2.com/display/Security/Security+Advisory+WSO2-2019-0633

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→