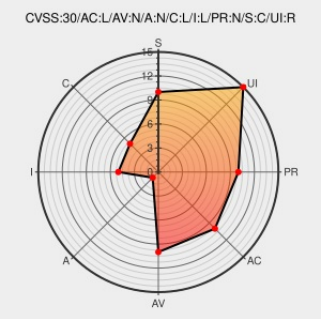
# CVE-2019-20437

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

Last Modified on: 11/10/2022 04:48:00 AM UTC

## CVE-2019-20437

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, WSO2 IS as Key Manager 5.7.0, and WSO2 Identity Server 5.8.0. When a custom claim dialect with an XSS payload is configured in the identity provider basic claim configuration, that payload gets executed, if a user picks up that dialect's URI as the provisioning claim in the advanced claim configuration of the same Identity Provider. The attacker also needs to have privileges to log in to the management console, and to add and update identity provider configurations.

CVE-2019-20437 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 6.1 - MEDIUM

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

### CVSS2 Score: 4.3 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | PARTIAL | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| CVE-2019-20437 - Stored Cross-Site Scripting | [illegible] | [illegible] MISC cybersecurityworks.com/zerodays/cve-2019 |

| | | |
|---|---|---|
| CVE-2019-20437 - Stored Cross-Site Scripting (XSS) in WSO2 Product | cybersecurityworks.com<br>text/html | MISC cybersecurityworks.com/zerodays/cve-2019-20437-wso2.html |
| Security Advisory WSO2-2019-0635 - WSO2 Platform Security - WSO2 Documentation | Vendor Advisory<br>docs.wso2.com<br>text/html | MISC docs.wso2.com/display/Security/Security+Advisory+WSO2-2019-0635 |
| Stored Cross Site Scripting (XSS) in "malicious dialect URI" on WSO2 Product - (WSO2 Identity Server version 5.7.0) · Issue #20 · cybersecurityworks/Disclosed · GitHub | Exploit<br>Third Party Advisory<br>github.com<br>text/html | MISC github.com/cybersecurityworks/Disclosed/issues/20 |



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 |
| Application | Wso2 | Identity Server | 5.7.0 | All | All | All |
| Application | Wso2 | Identity Server | 5.8.0 | All | All | All |
| Application | Wso2 | Identity Server | 5.7.0 | All | All | All |
| Application | Wso2 | Identity Server | 5.8.0 | All | All | All |

- cpe:2.3:a:wso2:api_manager:2.6.0:*:*:*:*:*:*:*
- cpe:2.3:a:wso2:api_manager:2.6.0:*:*:*:*:*:*:*
- cpe:2.3:a:wso2:identity_server:5.7.0:*:*:*:*:*:*:*
- cpe:2.3:a:wso2:identity_server:5.8.0:*:*:*:*:*:*:*
- cpe:2.3:a:wso2:identity_server:5.7.0:*:*:*:*:*:*:*
- cpe:2.3:a:wso2:identity_server:5.8.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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