



CVE-2018-20737

Published on: 03/18/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:36 PM UTC

CVE-2018-20737

[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 2.1.0 and 2.6.0. Reflected XSS exists in the carbon part of the product.

CVE-2018-20737 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	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-2018-20737 - Excellium Services	Patch Third Party Advisory www.excellium-services.com text/html	MISC www.excellium-services.com/cert-xlm-advisory/cve-2018-20737/

Encode variable in edit-oidc-claims-finish-ajaxprocessor.jsp by DMHP · Pull Request #978 · wso2-extensions/identity-inbound-auth-oauth · GitHub

Patch
Third Party Advisory
github.com
text/html

 **CONFIRM**
github.com/wso2-extensions/identity-inbound-auth-oauth/pull/978/files

Security Patch Releases

Patch
Third Party Advisory
Vendor Advisory
wso2.com
text/html

 **CONFIRM**
wso2.com/security-patch-releases/api-manager

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
Application	Wso2	Identity Server	5.7.0	All	All	All
Application	Wso2	Identity Server	5.7.0	All	All	All
Application	Wso2	Identity Server As Key Manager	5.7.0	All	All	All
Application	Wso2	Identity Server As Key Manager	5.7.0	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:5.7.0:*****:						
cpe:2.3:a:wso2:identity_server_as_key_manager:5.7.0:*****:						
cpe:2.3:a:wso2:identity_server_as_key_manager:5.7.0:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

CVE, CWE, and OVAL are registered 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](#)