Security Advisory for WSO2 API Manager

WSO2-2018-0369

31-07-2018

Severity : Medium

CVSS Score : 5.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L)

AFFECTED PRODUCTS

WSO2 API Manager	2.0.0 , 2.1.0

OVERVIEW

Potential XML External Entity (XXE) vulnerabilities have been identified in jaggery module sso.

DESCRIPTION

It was identified that in jaggery sso module secure parsing features have not been enabled in the XML parsers to prevent XXE attacks.

IMPACT

The XXE attacks can affect any trusted system respective to the machine where the parser is located. This attack may result in disclosing local files, denial of service, server-side request forgery, port scanning and other system impacts on affected systems.

SOLUTION

The recommended solution is to apply the provided patch/update to the affected versions of the products.

For WSO2 Update Manager (WUM) Supported Products

Please use WUM to update the following products. Patches can be used in case WUM is not applicable.

Code	Product	Version
AM	WSO2 API Manager	2.0.0 2.1.0

For Patch Supported Products

Apply the following patches based on your product version by following the instructions in the README file. Please use your WSO2 support credentials to access the patch links.

WSO2-CARBON-PATCH-4.4.0-2032 Download here

Please download the relevant patches based on the products you use following the matrix below.

Code	Product	Version	Patch
AM	WSO2 API Manager	2.0.0	WSO2-CARBON-PATCH-4.4.0-2032

NOTES

We have already tested these updates/patches in-house. However, we strongly recommend you to test this in your development/test environments before applying to the production setups.

Thanks,

WSO2 Team