Security Advisory for Multiple WSO2 Products

WSO2-2018-0426

31-07-2018

Severity : High

CVSS Score : CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:H

AFFECTED PRODUCTS

WSO2 API Manager	1.10.0 , 1.9.1 , 2.0.0 , 2.1.0 , 2.2.0
WSO2 API Microgateway	2.2.0
WSO2 IS as Key Manager	5.3.0 , 5.5.0

OVERVIEW

Application validation issue in the APIM store when subscription creation/deletion.

DESCRIPTION

This address an application validation issue when the API subscription creation/deletion is happening. The parameter applicationId which is in the API subscription creation/deletion request can be manipulated arbitrarily. Therefore API applications can be subscribed and unsubscribed to any application, even if the application does not support the logged in user.

IMPACT

Any user in the store can unsubscribe all the applications to the APIs and make the services unavailable to the API consumer applications.

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 2.2.0
AM-Micro-GW	WSO2 API Microgateway	2.2.0
IS KM	WSO2 IS as Key Manager	5.3.0 5.5.0

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-4.2.0-2256	Download here
WSO2-CARBON-PATCH-4.4.0-2609	Download here
WSO2-CARBON-PATCH-4.4.0-2618	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	1.10.0	WSO2-CARBON-PATCH-4.4.0-2609
		1.9.1	WSO2-CARBON-PATCH-4.2.0-2256
		2.0.0	WSO2-CARBON-PATCH-4.4.0-2618

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