Security Advisory for Multiple WSO2 Products

WSO2-2018-0384

31-07-2018

Severity : Medium

CVSS Score : 4.8 (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N)

AFFECTED PRODUCTS

WSO2 API Manager Analytics	2.0.0
WSO2 Data Analytics Server	3.0.0 , 3.0.1 , 3.1.0
WSO2 Enterprise Integrator	6.0.0 , 6.1.0 , 6.1.1
WSO2 Enterprise Service Bus Analytics	5.0.0
WSO2 Identity Server Analytics	5.2.0 , 5.3.0 , 5.4.0 , 5.4.1

OVERVIEW

A potential HTML/JS/XSS injection vulnerability has been identified in Activity Explorer Dashboard and Scripts Dashboard components.

DESCRIPTION

The HTML/JS/XSS injection vulnerability is identified in Activity Explorer application when adding search expression for searching and in Script Dashboard when adding spark scripts.

IMPACT

This vulnerability can lead to HTML injection attacks, reflects the attack back to the user's browser and will execute the injected code, which may generate malicious page results that will mislead the victim or harm

otherwise.

SOLUTION

The recommended solution is to apply the provided patch/update which encodes HTML for proper viewing, 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-Analytics	WSO2 API Manager Analytics	2.0.0
DAS	WSO2 Data Analytics Server	3.1.0
EI	WSO2 Enterprise Integrator	6.0.0 6.1.0 6.1.1
ESB-Analytics	WSO2 Enterprise Service Bus Analytics	5.0.0
IS-Analytics	WSO2 Identity Server Analytics	5.2.0 5.3.0 5.4.0 5.4.1

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-4.4.0-2309   Download here

WSO2-CARBON-PATCH-4.4.0-2311   Download here

WSO2-CARBON-PATCH-4.4.0-2312   Download here

WSO2-CARBON-PATCH-4.4.0-2313	Download here
WSO2-CARBON-PATCH-4.4.0-2314	Download here
WSO2-CARBON-PATCH-4.4.0-2315	Download here

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

Code	Product	Version	Patch
AM-Analytics	WSO2 API Manager Analytics	2.0.0	WSO2-CARBON-PATCH-4.4.0-2313
DAS	WSO2 Data Analytics Server	3.0.0	WSO2-CARBON-PATCH-4.4.0-2312
		3.0.1	WSO2-CARBON-PATCH-4.4.0-2311
		3.1.0	WSO2-CARBON-PATCH-4.4.0-2309
ESB-Analytics	WSO2 Enterprise Service Bus Analytics	5.0.0	WSO2-CARBON-PATCH-4.4.0-2314
IS-Analytics	WSO2 Identity Server Analytics	5.2.0	WSO2-CARBON-PATCH-4.4.0-2315

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