Security Advisory

Platform Security

Security Advisory for WSO2 Governance Regis

WSO2-2017-0238

31-07-2018

Severity : High

AFFECTED PRODUCTS

WSO2 API Manager	2.0.0 , 2.1.0
WSO2 API Manager Analytics	2.0.0 , 2.1.0
WSO2 Complex Event Processor	4.0.0 , 4.1.0
WSO2 Data Analytics Server	3.0.0 , 3.0.1
WSO2 Enterprise Service Bus Analytics	5.0.0
WSO2 Identity Server Analytics	5.3.0
WSO2 IoT Server	3.0.0

OVERVIEW

A potential Reflected Cross-Site Scripting (XSS) vulnerability has been identified in the Event Tracer component c Management Console.

DESCRIPTION

A reflected XSS attack could be performed in the Event Tracer of the Management Console by sending an HTTP C with a harmful request parameter. Additonally, auto-completion has not been turned off for the password form fiel Event Publisher" UI.

IMPACT

An attacker can trick a privileged user to click a crafted URL via email, IM or a neutral web site, then the attacker

browser to get redirected to a malicious website, make changes in the UI of the web page, retrieve information fror browser or harm otherwise. However, since all the session related sensitive cookies are set with httpOnly flag and j session hijacking or similar attacks would not be possible. Since password auto-complete has not been turned off, u decide to save credentials in browser which could lead to credential exposure in a shared computing environment.

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
AM-Analytics	WSO2 API Manager Analytics	2.0.0 2.1.0
ESB-Analytics	WSO2 Enterprise Service Bus Analytics	5.0.0
IS-Analytics	WSO2 Identity Server Analytics	5.3.0

For Patch Supported Products

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

WSO2-CARBON-PATCH-4.4.0-1388	Download here
WSO2-CARBON-PATCH-4.4.0-1389	Download here
WSO2-CARBON-PATCH-4.4.0-1390	Download here
WSO2-CARBON-PATCH-4.4.0-1391	Download here
WSO2-CARBON-PATCH-4.4.0-1392	Download here
WSO2-CARBON-PATCH-4.4.0-1393	Download here
WSO2-CARBON-PATCH-4.4.0-1396	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.(
AM-Analytics	WSO2 API Manager Analytics	2.0.0	WSO2-CARBON-PATCH-4.4.(
CEP	WSO2 Complex Event Processor	4.0.0	WSO2-CARBON-PATCH-4.4.(
		4.1.0	WSO2-CARBON-PATCH-4.4.(
DAS	WSO2 Data Analytics Server	3.0.0	WSO2-CARBON-PATCH-4.4.(
		3.0.1	WSO2-CARBON-PATCH-4.4.(
ESB-Analytics	WSO2 Enterprise Service Bus Analytics	5.0.0	WSO2-CARBON-PATCH-4.4.(
IOT	WSO2 IoT Server	3.0.0	WSO2-CARBON-PATCH-4.4.(

NOTES

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

Thanks,

WSO2 Team