Security Advisory

WSO2-2018-0230

Scope: Multiple WSO2 Products
Date: 31-07-2018
Severity: Medium
CVSS Score : 4.5 (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:N/A:N)
Email: security@wso2.com

Platform Security

Affected Products

WSO2 API Manager : 1.10.0 , 2.1.0
WSO2 App Manager : 1.2.0
WSO2 Governance Registry : 5.0.0 , 5.0.1 , 5.1.0 , 5.2.0 , 5.3.0
WSO2 IoT Server : 3.0.0

Overview

A potential Cross-Site Scripting (XSS) vulnerability has been identified in API Manager Management console.

Description

This vulnerability is discovered in the message dialog page of the Management Console. XSS allows an attacker to execute malicious code (scripts) against the web browser of the user. Also XXE and SSRF vulnerabilities have been identified along with this.

Impact

By leveraging an XSS attack, an attacker can make the browser get redirected to a malicious website, make changes in the UI of the web page, retrieve information from the browser or harm otherwise. However, since the session cookies are protected with httpOnly flag, session hijacking is not possible.

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	2.1.0

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-4.4.0-1050	Download here
WSO2-CARBON-PATCH-4.4.0-1054	Download here
WSO2-CARBON-PATCH-4.4.0-1057	Download here

WSO2-CARBON-PATCH-4.4.0-1059	Download here
WSO2-CARBON-PATCH-4.4.0-1060	Download here
WSO2-CARBON-PATCH-4.4.0-1062	Download here
WSO2-CARBON-PATCH-4.4.0-1071	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-4.4.0-1050
APPM	WSO2 App Manager	1.2.0	WSO2-CARBON-PATCH-4.4.0-1059
GREG	WSO2 Governance Registry	5.0.0	WSO2-CARBON-PATCH-4.4.0-1050
		5.0.1	WSO2-CARBON-PATCH-4.4.0-1054
		5.1.0	WSO2-CARBON-PATCH-4.4.0-1057
		5.2.0	WSO2-CARBON-PATCH-4.4.0-1060
		5.3.0	WSO2-CARBON-PATCH-4.4.0-1071
IOT	WSO2 IoT Server	3.0.0	WSO2-CARBON-PATCH-4.4.0-1062

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 Platform Security