Security Advisory for WSO2 Governance Registry

WSO2-2017-0231

31-07-2018

Severity : Medium

AFFECTED PRODUCTS

WSO2 API Manager	1.10.0 , 1.9.1 , 2.0.0 , 2.1.0
WSO2 API Manager Analytics	2.0.0 , 2.1.0
WSO2 App Manager	1.1.0 , 1.2.0
WSO2 Application Server	5.3.0
WSO2 Business Process Server	3.5.0 , 3.5.1 , 3.6.0
WSO2 Business Rules Server	2.2.0
WSO2 Complex Event Processor	4.0.0 , 4.1.0 , 4.2.0
WSO2 Data Analytics Server	3.0.0 , 3.0.1 , 3.1.0
WSO2 Data Services Server	3.5.0 , 3.5.1
WSO2 Enterprise Integrator	6.0.0
WSO2 Enterprise Service Bus	4.9.0 , 5.0.0
WSO2 Enterprise Service Bus Analytics	5.0.0
WSO2 Governance Registry	5.0.0 , 5.0.1 , 5.1.0 , 5.2.0 , 5.3.0 , 5.4.0
WSO2 IS as Key Manager	5.2.0 , 5.3.0
WSO2 Identity Server	5.1.0 , 5.2.0 , 5.3.0
WSO2 Identity Server Analytics	5.2.0 , 5.3.0
WSO2 Machine Learner	1.0.0 , 1.1.0 , 1.2.0
WSO2 Message Broker	3.0.0 , 3.1.0

OVERVIEW

A potential clickjacking vulnerability has been identified in the WSO2 kernel.

DESCRIPTION

Some security headers (eg: X-FRAME-OPTIONS) get duplicated in the response headers of WSO2 servers due to the introduction of HttpHeaderSecurityFilter, which would open up clickjacking vulnerability when using several older versions of browsers.

IMPACT

By leveraging clickjacking attack, an attacker could trick a user into clicking a button, a link or a picture, etc. that the web user did not intend to click, typically by overlaying the web page with an iframe. This malicious technique can potentially expose confidential information or, less commonly, take control of the user's computer.

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
CEP	WSO2 Complex Event Processor	4.2.0
DAS	WSO2 Data Analytics Server	3.1.0
DSS	WSO2 Data Services Server	3.5.1
EI	WSO2 Enterprise Integrator	6.0.0

ESB	WSO2 Enterprise Service Bus	4.9.0 5.0.0
ESB-Analytics	WSO2 Enterprise Service Bus Analytics	5.0.0
GREG	WSO2 Governance Registry	5.4.0
IS KM	WSO2 IS as Key Manager	5.2.0 5.3.0
IS	WSO2 Identity Server	5.2.0 5.3.0
IS-Analytics	WSO2 Identity Server Analytics	5.2.0 5.3.0

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-4.2.0-2170	Download here
WSO2-CARBON-PATCH-4.4.0-1039	Download here
WSO2-CARBON-PATCH-4.4.0-1040	Download here
WSO2-CARBON-PATCH-4.4.0-1041	Download here
WSO2-CARBON-PATCH-4.4.0-1427	Download here
WSO2-CARBON-PATCH-4.4.0-1428	Download here
WSO2-CARBON-PATCH-4.4.0-1429	Download here
WSO2-CARBON-PATCH-4.4.0-1435	Download here
WSO2-CARBON-PATCH-4.4.0-1436	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-4.4.0-1429
		1.9.1	WSO2-CARBON-PATCH-4.2.0-2170
		2.0.0	WSO2-CARBON-PATCH-4.4.0-1041
AM-Analytics	WSO2 API Manager Analytics	2.0.0	WSO2-CARBON-PATCH-4.4.0-1041
APPM	WSO2 App Manager	1.1.0	WSO2-CARBON-PATCH-4.2.0-2170
		1.2.0	WSO2-CARBON-PATCH-4.4.0-1041
AS	WSO2 Application Server	5.3.0	WSO2-CARBON-PATCH-4.4.0-1436
BPS	WSO2 Business Process Server	3.5.0	WSO2-CARBON-PATCH-4.4.0-1436
		3.5.1	WSO2-CARBON-PATCH-4.4.0-1428
		3.6.0	WSO2-CARBON-PATCH-4.4.0-1040
BRS	WSO2 Business Rules Server	2.2.0	WSO2-CARBON-PATCH-4.4.0-1429
CEP	WSO2 Complex Event Processor	4.0.0	WSO2-CARBON-PATCH-4.4.0-1436
		4.1.0	WSO2-CARBON-PATCH-4.4.0-1429
		4.2.0	WSO2-CARBON-PATCH-4.4.0-1039
DAS	WSO2 Data Analytics Server	3.0.0	WSO2-CARBON-PATCH-4.4.0-1435
		3.0.1	WSO2-CARBON-PATCH-4.4.0-1429
		3.1.0	WSO2-CARBON-PATCH-4.4.0-1039
DSS	WSO2 Data Services Server	3.5.0	WSO2-CARBON-PATCH-4.4.0-1435
		3.5.1	WSO2-CARBON-PATCH-4.4.0-1039
ESB	WSO2 Enterprise Service Bus	4.9.0	WSO2-CARBON-PATCH-4.4.0-1436
		5.0.0	WSO2-CARBON-PATCH-4.4.0-1040

ESB-Analytics	WSO2 Enterprise Service Bus Analytics	5.0.0	WSO2-CARBON-PATCH-4.4.0-1040
GREG	WSO2 Governance Registry	5.0.0	WSO2-CARBON-PATCH-4.4.0-1436
		5.0.1	WSO2-CARBON-PATCH-4.4.0-1436
		5.1.0	WSO2-CARBON-PATCH-4.4.0-1436
		5.2.0	WSO2-CARBON-PATCH-4.4.0-1427
		5.3.0	WSO2-CARBON-PATCH-4.4.0-1041
IS KM	WSO2 IS as Key Manager	5.2.0	WSO2-CARBON-PATCH-4.4.0-1039
IS	WSO2 Identity Server	5.1.0	WSO2-CARBON-PATCH-4.4.0-1429
		5.2.0	WSO2-CARBON-PATCH-4.4.0-1039
IS-Analytics	WSO2 Identity Server Analytics	5.2.0	WSO2-CARBON-PATCH-4.4.0-1039
ML	WSO2 Machine Learner	1.0.0	WSO2-CARBON-PATCH-4.4.0-1436
		1.1.0	WSO2-CARBON-PATCH-4.4.0-1429
		1.2.0	WSO2-CARBON-PATCH-4.4.0-1039
MB	WSO2 Message Broker	3.0.0	WSO2-CARBON-PATCH-4.4.0-1435
		3.1.0	WSO2-CARBON-PATCH-4.4.0-1429

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