WSO2 ESB Disclosures

Version 5.0.0

Environment:

- WSO2 ESB 5.0.0
- OpenJDK 1.8.0_252
- Ubuntu Linux

Findings:

1. MAL-007: XXE in Local Registry Entries

Description:
An inline XML External Entity (XXE) attack was identified in the WSO2 ESB “Local Entities” tool. This XXE can be exploited by using malicious XML Entity elements in the “Inlined XML Entity” Editor.

Proof of Concept:
In this scenario we will create a new “Inlined XML Entity” called “test”.

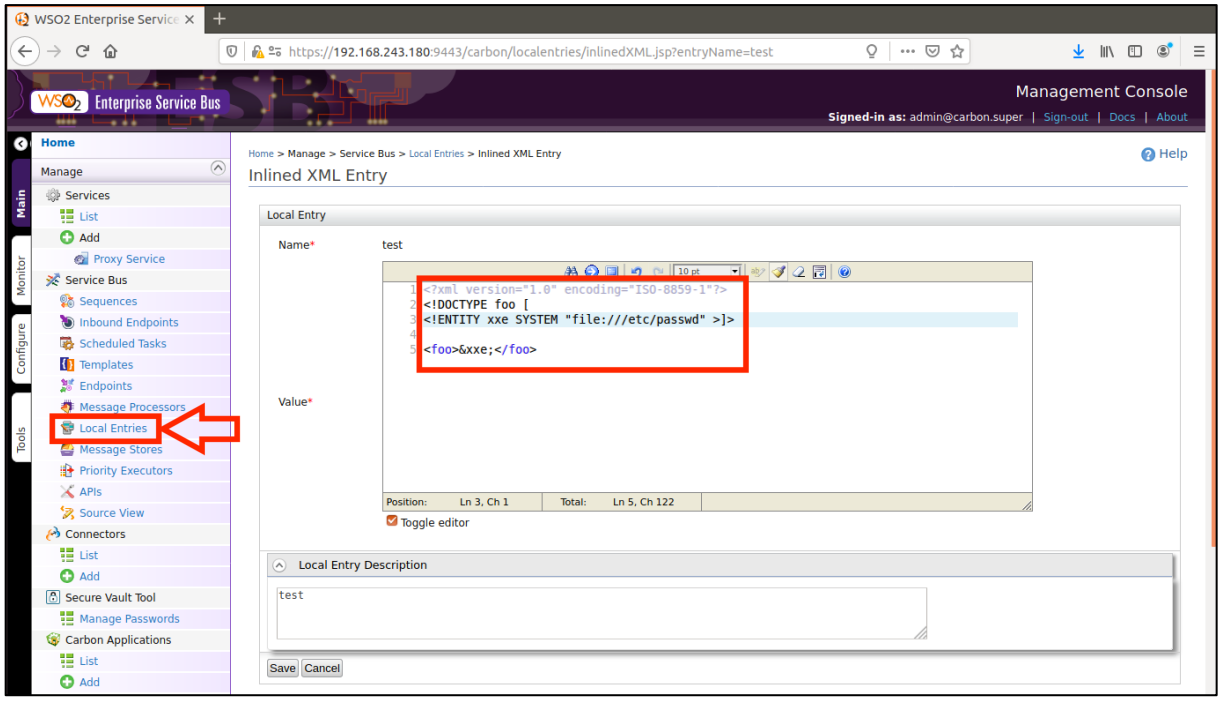
Note: Editing an already existing entity may also be a valid scenario.

XXE Payload:

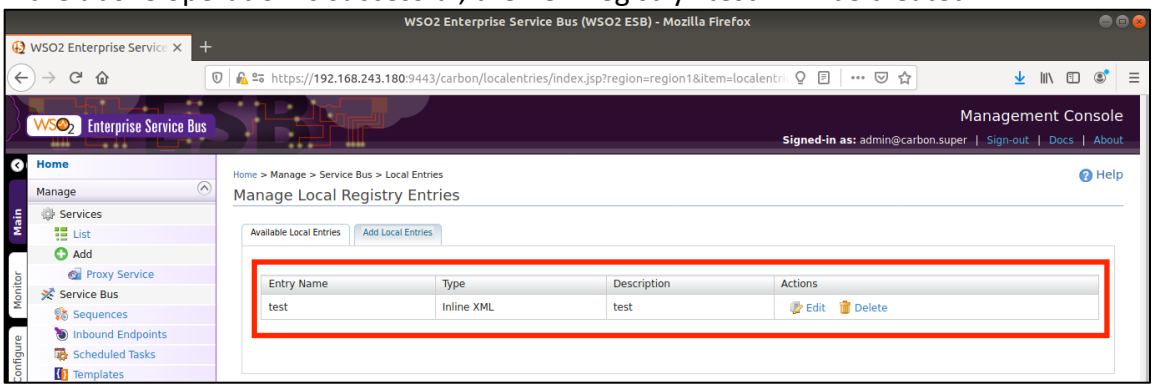
```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>

<foo>&xxe;</foo>
```

Web View:



If the above operation is successful, the new registry “test” will be created:



Now if the “Edit” button is pressed, we will see the content of the exfiltrated file (in this case “/etc/passwd”) in the editor: