CVE-2020-1938 Apache Tomcat AJP Request Injection and potential Remote Code Execution

2020-03-02 - Steef | ESET Nederland - Reacties (0) - Customer Advisories

Issue:

- You are using an Apache Tomcat version affected by the vulnerability CVE-2020-1938
- Tomcat 9.0.22 distributed with ESMC 7.1 is also affected by the vulnerability

Details

See the vulnerability description here: CVE-2020-1938.

The affected Apache Tomcat versions are:

- 9.0.0.M1 - 9.0.0.30
- 8.5.0 - 8.5.50
- 7.0.0 - 7.0.99

In the affected versions, the Apache Tomcat treats AJP connections as having higher trust than other connections. ESET Security Management Center and ESET Remote Administrator are not using the AJP connector.

Solution

There are three possible solutions to this issue. You need to apply only one of them:

Solution 1: Update the Apache Tomcat version using the all-in-one installer

Use the ESMC 7.1.27.1 all-in-one installer for Windows to upgrade your Apache Tomcat. See the KB article with detailed steps.

Solution 2: Block the AJP port

Block the*Apache JServ Protocol*(AJP) port 8009 for incoming connections on your firewall:

Windows users

Windows Server usually blocks the port by default, but you can create a new explicit rule to block the port. If you manage your firewall with a security product, use the product to create a rule to block inbound connections on port 8009.

You can check if the port is open by using the following command:

```
netstat -ano | findstr 8009
```

Linux users

Make sure to block the port 8009 using your security product or via Linux utility iptables.

If you use iptables, run following command as superuser:

```
iptables -A INPUT -j DROP --destination-port 8009
```

```
You can check if the port is open using the following command:
```

```
ss -a | grep 8009
```

ERA / ESMC Virtual Appliance users

No action is required. The firewall on the Appliance is pre-set to block all connections not related to ESET products.

Solution 3: Disable the AJP connector

Disable the AJP connector in the Tomcat configuration. Use this solution if you need to continue using port 8009.

- Open the Tomcat configuration for editing:

Windows: `C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\conf\server.xml`

Linux: `/etc/tomcat9/server.xml`

- `Search for "8009" and comment out the line about AJP protocol:`

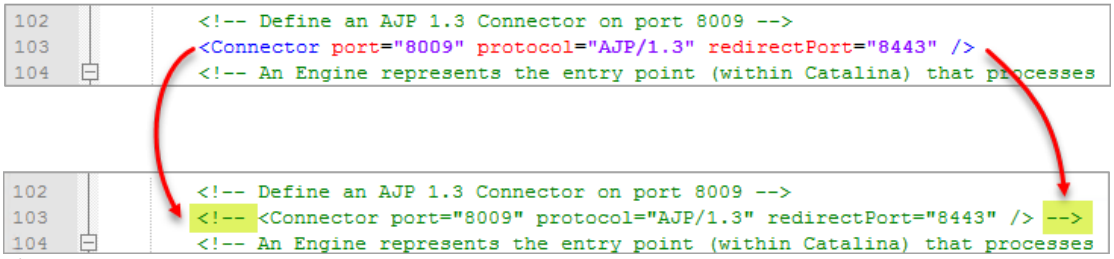


Figure 1-1

- Save the changes in the file.
- Restart the Apache Tomcat service.