Add detection rules in ESET Enterprise Inspector for Log4j 2 vulnerability

Steef | ESET Nederland - 2022-03-03 - Comments (0) - ESET INSPECT (ESET Enterprise Inspector)

Issue

- Import detection rules into ESET Enterprise Inspector (EEI) to detect the Log4j 2 vulnerability

Solution

The two Log4Shell rules below are designed to detect the log4j2 exploit. The rules use an experimental feature not fully supported by EEI, so detection may not work each time. For example, if a detection has already been reported on the network layer, EEI will not detect the exploit again. ESET recommends executing the two rules below as a task using the Rerun task option.

- Possible Log4Shell (CVE-2021-44228) exploitation [D0532a]
- Possible Log4Shell (CVE-2021-44228) exploitation [D0532b]

The two rules below are for the general exploitation of Java Runtime, for example, CVE-2021-44228. These general rules may generate some false positives for legitimate Java applications.

- Potential Java Runtime exploitation [E0461]
- Java Runtime executing suspicious script/command interpreter [E0462]

Import rules into EEI

1. Download and unzip the detection rules file.
2. Open ESET Enterprise Inspector.
3. Click **Admin**.
4. Click **Detection Rules**.
5. Click **Import** to select the import file.
6. Select the file and click **Open**.
7. Repeat steps 5-6 for each file.