EEI Detection Rules Pack Update Announcement: Log4j Critical Vulnerability

2021-12-16 - Danny | ESET Nederland - Reacties (0) - Customer Advisories

The recently discovered Log4j remote code execution vulnerability has affected organizations, our customers and their IT teams, around the globe and as cybersecurity professionals we need to ensure their safety.

Our Research & Threat Analysis team has responded rapidly and created a package of 4 rules for detection of Log4j exploitation and more general Java runtime exploitation.

We recommend to import these rules (the import procedure is very simply done from the Admin-->Detection Rules--> Import section of EI as described here).

These rules will also be included in the upcoming hotfix for EEI 1.6, but we are making them available right now:

- Possible Log4Shell (CVE-2021-44228) exploitation [D0532a]
- Possible Log4Shell (CVE-2021-44228) exploitation [D0532b]
- Potential Java Runtime exploitation [E0461]
- Java Runtime executing suspicious script/command interpreter [E0462]

The first two rules are designed to detect the exploit itself so the false positives count should be absolutely minimal. Use the re-run task for a retrospective threat hunt .

The last two rules are focused on more general types of cases, general exploitation of Java Runtime i.e. not only by CVE-2021-44228. That means that those rules may generate occasional false positives for the cases when some legitimate Java application is executing system components which may indicate an attacker's activity. We have tested these rules to not have an excess number of false positives, but in case you will observe unusual amount of FPs in your environments - please report them back to us.

The rule pack itself can be found here.