Log4J Vulnerabilities - Trend Micro Resolutions (Updated to 20 Dec 2021)

The information provided below is referred from https://success.trendmicro.com/solution/000289940 and https://log4j tester.trendmicro.com/.

- **CVE Number**

  2021-44228

- **Discovery Date**

  No Information

- **Threat Level**

  High

- **Response to Log4j**

The challenge with this vulnerability is widespread use of this particular logging utility in many enterprise and cloud applications. JDNI lookups support multiple protocols, but based on analysis so far, exploitability depends on the Java versions and configurations. From a practical standpoint, just because a server has implemented an affected version of Log4j 2, it does not automatically mean it is vulnerable depending on its configuration.

- **Affected Trend Micro Products**

At this moment (12-16-2021), there is no product to be affected by the Log4j vulnerabilities.
Trend Micro Protection Products
Trend Micro has released some supplementary rules, filters and detection protection that may help provide additional protection and detection of malicious components associated with this attack servers that have not already been compromised or against further attempted attacks.

1. **Trend Micro Cloud One**

    Apply the following – Workload Security and Deep Security IPS Rules:

    1. Rule 1011242 – Log4j Remote Code Execution Vulnerability (CVE-2021-44228)
    2. Rule 1005177 – Restrict Java Bytecode File (Jar/Class) Download
    3. Rule 1008610 – Block Object-Graph Navigation Language (OGNL) Expressions Initiation In Apache Struts HTTP Request
    4. LI Rule 1011241 – Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)

2. **Trend Micro Deep Discovery Inspector(DDI) Rules**
    Apply the following (DDI) Rules:

1. Rule 4280: HTTP_POSSIBLE_USERAGENT_RCE_EXPLOIT_REQUEST Rule 4641: CVE-2021-44228 – OGNL EXPLOIT – HTTP(REQUEST)
2. Rule 4642: POSSIBLE HTTP HEADER OGNL EXPRESSION EXPLOIT – HTTP(REQUEST)
3. Rule 4643: POSSIBLE HTTP BODY OGNL EXPRESSION EXPLOIT – HTTP (REQUEST) – Variant 2

3. **Trend Micro Cloud One – Network Security and TippingPoint Filters**

Filter 40627 : HTTP: JNDI Injection in HTTP Header or URI

4. Trend Micro Log4j Vulnerability Scanner

Trend Micro Research has created a quick web-based scanning tool that can help users and administrators identify server applications that may be affected but the Log4Shell vulnerability.

The tool can be found at: https://log4j-tester.trendmicro.com/.