Log4J Vulnerabilities - SOTI Resolutions (Updated to 10 Dec 2021)

The information provided below is referred from https://discussions.soti.net/articles/log4j-vulnerability-log4shell-important-information-you-should-know.

- **CVE Number**

  2021-44228

- **Discovery Date**

  Dec 10, 2021

- **Threat Level**

  High

- **Response to Log4j**

A vulnerability was recently announced in the Log4j library. The vulnerability, known as Log4Shell (CVE-2021-44228), has been actively investigated by SOTI's Security & Compliance Team since Friday, December 10, 2021. The SOTI ONE Platform makes indirect use of this library, and to date, our investigations have determined no exploitable path to the vulnerability within the SOTI ONE Platform.

- **SOTI Usage of Log4j**

The SOTI ONE Platform products that make use of Log4j do so indirectly.

The SOTI development team has not found any way in which this can be exploited in the SOTI ONE Platform. A standard programming practice at SOTI is to sanitize all inputs.

This means that our products are safeguarded against the underlying vulnerability, even if no further action is taken.

SOTI MobiControl, SOTI Central and SOTI Snap make indirect use of the Log4j library through Elasticsearch.

According to Elasticsearch:

> The Remote Code Execution (RCE) vulnerability is not exploitable.
> The information leak via DNS is only susceptible when running JDK8 or below.

As stated above, this cannot be exploited through SOTI MobiControl as we sanitize our inputs.