Log4j vulnerability and ELK impact

Ensuring quality on schedule

Log4j vulnerability

December 10th the public disclosure of the Apache Log4j vulnerability - **CVE-2021-44228** affecting several **Java based** custom and commercial applications

- Exploited by nation state attackers and ransomware groups, such as APT35 and Hafnium
- Affected versions **2.0-beta9 through 2.14.1** of Log4j2
- Google using **Open Source Insights** estimates that over **35,000 packages** (over **8% of Maven** Central repository) have been impacted

Incomplete and resulted in a potential DoS and data exfiltration vulnerability, logged as **CVE-2021-45046**.

Fix new vulnerability was also found **vulnerable** leading to a new **CVE-2021-45105**

Is a solution to the vulnerability problem.

Impact on ELK

All releases of **Elasticsearch 5.0 to 7.16.0 are using a vulnerable Log4j2 version**

Elasticsearch	JDK	RCE	Leak	Action required	Protection in place
≥ 7.16.2	any	–	–	–	Log4j 2.17.0
7.16.1	any	–	–	–	JNDILookup class removed and log4j2.formatMsgNoLookups=true
7.0.0 – 7.16.0	≥ 9	–	–	– [1]	Java Security Manager and JVM default
7.0.0 – 7.16.0	< 9	–	✸	Set formatMsgNoLookups	Java Security Manager
6.8.22	any	–	–	–	Log4j 2.17.0
6.8.21	any	–	–	–	JNDILookup class removed and log4j2.formatMsgNoLookups=true
6.0.0 – 6.8.20	≥ 9	–	–	– [1]	Java Security Manager and JVM default
6.4.0 – 6.8.20	< 9	–	✸	Set formatMsgNoLookups	Java Security Manager
6.0.0 – 6.3.2	< 9	–	✸	Remove JNDILookup class	Java Security Manager
≥ 5.6.11	any	✸	✸	Set formatMsgNoLookups	–
5.0.0 – 5.6.10	any	✸	✸	Remove JNDILookup class	–
< 5.0.0	any	–	–	–	Log4j 1.x

*RCE (Remote Code Execution), *Leak – Exposes Log4jlookups like environment variables

ELK Mitigation Plan Options

Upgrade to Elasticsearch ≥ 7.16.2 or ≥ 6.8.22 which has upgraded Log4j to 2.17.0.

- Elasticsearch **7.16.1 or 6.8.21, are also protected** against the three vulnerabilities. These versions have set -Dlog4j2.formatMsgNoLookups=true in the JVM options and remove the JndiLookup class, which cover all three vulnerabilities in the context of Elasticsearch
- If upgrade in not an option, apply the **JVM option log4j2.formatMsgNoLookups=true** if you are using Elasticsearch ≥ 6.4.0 or ≥ 5.6.11 for an additional layer of protection.
- For more details please go through this link - **https://xeraa.net/blog/2021_mitigate-log4j2-log4shell-elasticsearch/#what-does-that-mean-for-elasticsearch**