Vulnerabilidade da biblioteca Log4j e projetos Low-Code

Nas últimas semanas foi notificado uma vulnerabilidade identificada como **CVE-2021-44228** na biblioteca log4j-core-2x à 2-14, a equipe de segurança da Techne/Cronapp tomou conhecimento e constatou que os projetos exclusivamente **Low-code** do Cronapp não possuem essa biblioteca, **portant o não estão vulneráveis**, Leia mais.

Figura 1 - Biblioteca Log4j versão 2

Portanto, os projetos criados exclusivamente como **Low-code** estão livres dessa vulnerabilidade e podem ser validados da seguinte forma:

* Os comandos abaixo são para servidores Linux, use comando equivalente no Windows.

- Acesse seu servidor dentro do diretório do Tomcat e execute o comando abaixo, verá que não há a biblioteca mencionada:

```
find . -type f -iname log4j-core*.jar
```

- Acesse o site https://log4j-tester.trendmicro.com e siga as instruções informando a url do seu sistema.

Caso use projeto High-Code, certifique-se que não foi incluída essa biblioteca na sua aplicação, caso sim, proceda com uma das correções sugeridas:

* Os comandos abaixo são para servidores Linux, use comando equivalente no Windows;

1. Atualize para Log4j mais recente (acompanhe as novas vulnerabilidades publicadas);
2. Bloquear via WAF (caso possua um em seu ambiente *On Premises*);
3. Se você estiver usando o Log4j v2.10 ou superior e não puder atualizar, defina a propriedade JVM flag:

   ```
   -Dlog4j2.formatMsgNoLookups=true
   ```

   Além disso, uma variável de ambiente pode ser definida para essas mesmas versões afetadas (Log4j v2.10 ou superior):

   ```
   LOG4J_FORMAT_MSG_NO_LOOKUPS=true
   ```

4. Ou remova a classe `JndiLookup`, caso não utilize:

```
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup
/JndiLookup.class
```

5. Bloquear acesso ao servidor LDAP para o servidor de aplicação, caso seja possível.

Quer saber mais sobre essa vulnerabilidade? Acesse os links abaixo:

- https://gblogs.cisco.com/br/seguranca/nelsonbrito/do-que-se-trata-a-vulnerabilidade-apache-log4j/
- https://nvd.nist.gov/vuln/detail/CVE-2021-44228
- https://aws.amazon.com/pt/security/security-bulletins/AWS-2021-006/
- https://businessinsights.bitdefender.com/security-advisory-bitdefender-response-to-critical-0-day-apache-log4j2-vulnerability