第五章：**Log4Shell**

Log4Shellとは何か、およびコードをゼロディ脆弱性から守る方法を学ぶ

Log4Shellとは？

オープンソース

概要

Log4jとは？

まず、この脆弱性の影響を受けるパッケージである「log4j」について説明しましょう。Log4jとは、プログラミングライブラリ(つまり、あらかじめ作成されたコード)で、世界中の何百万ものコンピュータアプリケーションに使用されています。Log4jはオープンソースで無料で、2001年以来広く利用されています。Log4jは、アプリケーションでログの履歴を記録する目的でファイル/データベースに情報を出力するために使用されます。

Log4Shellとは？

Log4Shellは、Apacheソフトウェア財団が管理するlog4jユーティリティにて発見されたリモートコード実行(RCE)の脆弱性の通称です。具体的には、Log4Shellは[CVE-2021-44228]および関連する脆弱性を指します。

脆弱なバージョンのlog4jがアプリケーションで使用されている場合、攻撃者はこのアプリケーションをトリガーにし、攻撃者の管理下にあるホストにアクセスすることができます。そして、そこに配置されている悪意のあるコードをアプリケーションのサーバで展開し、攻撃者がアプリケーションやアプリケーションが置かれているサーバを制御することが可能になります。

Log4jのハッキングを開始するには、たった1つのWebリクエストで十分です。多くの場合、リクエストはユーザが認証される前に発生します。

[Log4j Contrastのデモ]

影響

Log4Shellは重大な脆弱性であり、攻撃者が標的に対して悪意のあるコードをリモートで実行する可能性があります。悪用された場合、データ漏洩、マルウェアのインストール、システムの完全な乗っ取りなど様々な影響に及ぶ可能性があります。

対策方法

Log4j2

Log4j2 を使用している方は、log4j-coreを利用可能な最新バージョンにアップグレードしてください。アップグレードできないバージョンでは、以下の方法でクラスパスからJNDI Lookupクラスを削除してください：

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

カスタムアプリケーションの場合は、ライブラリを更新して再ビルドし、アプリケーションを再デプロイすることをお勧めします。
ベンダーのアプリケーションについては、ベンダーから更新されたソフトウェアを入手してください。更新プログラムがなかったり、更新プログラムを適用しなかった場合、システムやデータがリモートから悪用される危険性が高くなります。

Log4j1

Log4j1が使用されていることが分かったら、推奨策に従い、log4j v2.17にアップグレードするか、ライブラリからJMSAppenderとSocketServerクラスを削除してください。削除を行うには、次のコマンドを実行します(パスにお使いのlog4jのバージョンを指定してください)：

```
Unset
zip -d log4j-1.x.x.jar org/apache/log4j/net/JMSAppender.class
```

```
Unset
zip -d log4j-1.x.x.jar org/apache/log4j/net/SocketServer.class
```

また、SCA(ソフトウェアコンポジション解析)やSBOM(ソフトウェア部品表)を作成できるセキュリティソリューションを活用して、アプリケーションがこのCVEに対して脆弱であるかを簡単に検出することもできます。Contrast Securityが提供するソリューションは完全な製品スィートであり、log4jやその他の脆弱なライブラリを検出するために使用できる、開発者向けの無料のCodeSecというツールもあります。SBOMは、どのアプリケーションが影響を受けるかを即座に把握でき、ユーザやセキュリティ担当が対策を講じることができる優れたインベントリです。
インベントリをまだ作成していない他のアプリケーションがあれば、確認することをお勧めします。SafeLog4Jなどのツールを使用して、そのようなアプリケーションを検査することができます。

おつかれさまでした！

Log4Shellとは何であるか、そしてお使いのシステムでそれにどう対策すべきかが、お分かり頂けたと思います。ここで学んだ新しい知識をうまく応用しながら、コーディングをしてください。これをあなたのネットワークで自由に共有してください。また、一般的な脆弱性に関する弊社のその他のレッスンも是非ご覧ください。
この学習モジュールに関して修正などがある場合は、こちらをクリックして、プルリクエストを作成してください！

関連記事:

ブログ:Log4Shell By The Numbers

ブログ:Log4Shell still an issue, but CodeSec audit can help