2021 年 12 月 14 日

サービス＆セキュリティ株式会社 e-Gate センター

注意喚起：Apache Log4j の脆弱性情報について

1. 概要

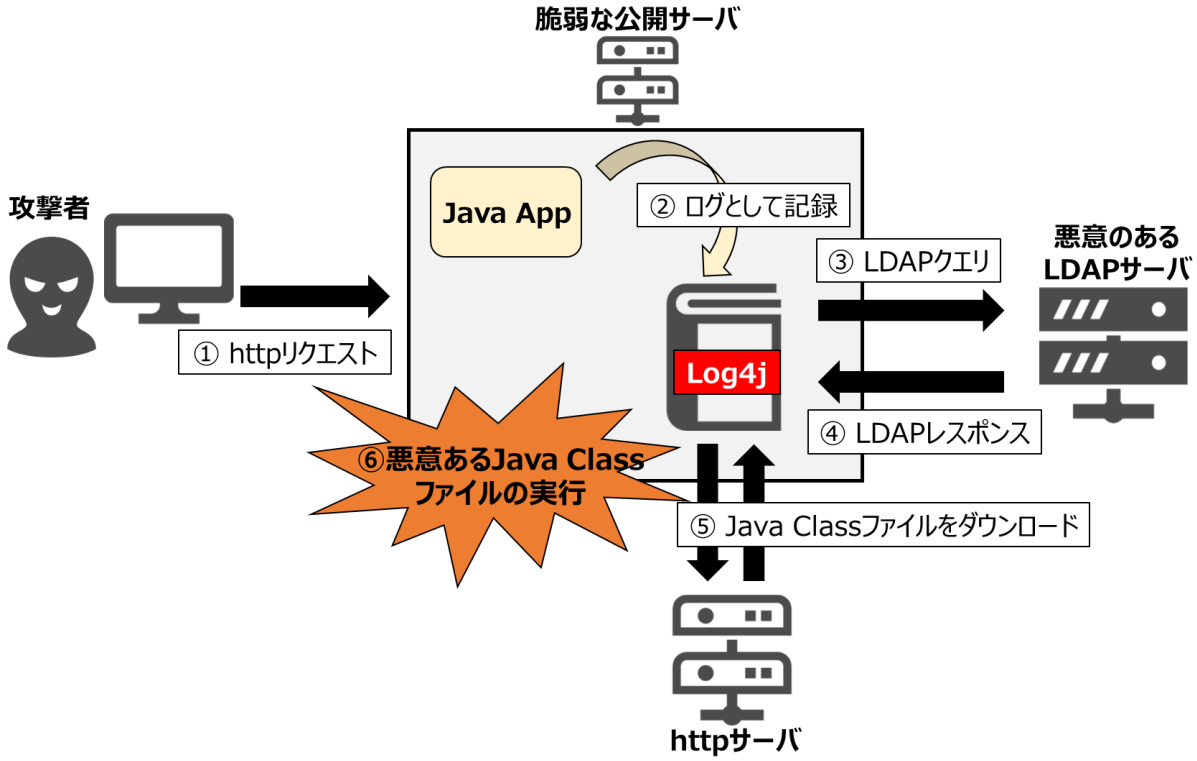
Java のログ出力ライブラリー「Apache Log4j」で、深刻な脆弱性（CVE-2021-44228）が存在することが報告されました。この脆弱性を悪用する攻撃が日本で確認されたとして 12 月 11 日には JPCERT コーディネーションセンター（JPCERT/CC）にて緊急で注意喚起が行われています。

Java は様々な場面で使われており、攻撃が容易であることから「Heartbleed」や「ShellShock」などと並ぶ深刻な脆弱性であるとも評価されており、対策済みのバージョンへのアップデートや回避策を至急実施する必要があります。

2. 脆弱性情報詳細

（1） 攻撃概要

「Apache Log4j」（以降は Log4j と記載）は、Java アプリケーションのログを出力するライブラリーであり、多数のアプリケーションに実装されているオープンソースのフレームワークです。Log4j にはログとして記録された文字列から、一部の文字列を変数として置換する Lookup と呼ばれる機能が存在します。これに含まれる JNDI（Java Name and Directory Interface）の Lookup 機能が悪用された場合、リモートから任意のコードが実行される恐れがあります。



【図 1】Apache Log4j の脆弱性を悪用した攻撃例

① 攻撃者は細工した文字列を含む http リクエストを送信。
② Log4j が Java App から細工された文字列をログとして保存。
③ JNDI を経由し、JNDI Lookup 機能によってログ内の文字を変数化することで LDAP クエリを送信。
④ 攻撃者の用意した LDAP サーバが悪意ある Java Class ファイルが配置された URL を応答。
⑤ Log4j が悪意ある Java Class ファイルをダウンロード
⑥ Log4j が悪意ある Java Class ファイルを実行

（2） 影響を受けるシステム

Apache Log4j 2.15.0 より前の 2 系のバージョン

Apache Log4j 1 系のバージョンは、Lookup 機能が含まれておらず、JMS Appender が有効でもクラス情報がデシリアライズされないため影響を受けないと報告されています。なお、1 系のバージョンはすでにサポートが終了しているため、本脆弱性に関わらず最新版へのアップデートを推奨いたします。

（3） 対策

すでに本脆弱性の悪用を試みる通信が確認されていることから影響を受けるシステムを利用している場合、速やかな対応が必要です。

A) 最新アップデート適用

The Apache Software Foundation から本脆弱性を修正したバージョンが公開されています。修正済みバージョンへアップデートすることが推奨されます。次のバージョン以降では、Lookup 機能がデフォルトで無効となっています。

- Apache Log4j 2.15.0

B) 回避策の実行

- Lookup 機能の無効化（Log4j バージョン 2.10 およびそれ以降で利用可）
  - Log4j を実行する Java 仮想マシンを起動時に「log4j2.formatMsgNoLookups」という JVM フラグオプションを指定する
  - 環境変数「LOG4J_FORMAT_MSG_NO_LOOKUPS」を「true」に設定する

- PatternLayout の変更（Log4j バージョン 2.7 およびそれ以降で利用可）
  - PatternLayout 構成から「%m{nolookups}」を指定することで、Lookup が実行されないようにする

- 特定 class の削除（Log4j バージョン 2.10 より前で利用可）
  - JndiLookup クラスをクラスパスから削除する

3. 参考情報

JPCERT/CC
Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210050.html

IPA
Apache Log4j の脆弱性対策について(CVE-2021-44228)
https://www.ipa.go.jp/security/ciadr/vul/alert20211213.html

JVNVU#96768815
Apache Log4j における任意のコードが実行可能な脆弱性
https://jvn.jp/vu/JVNVU96768815/

4. e-Gate の監視サービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。e-Gate のセキュリティ監視サービスをご活用いただきますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた「IT 運用のノウハウ」と最新のメソッドで構築した「次世代 SOC“e-Gate センター”」。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】
https://www.ssk-kan.co.jp/e-gate/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。
　リンク先のコンテンツは予告なく、変更、削除される場合があります。
※掲載した会社名、システム名、製品名は一般に各社の登録商標 または商標です。

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp