2022 年 1 月 30 日

サービス＆セキュリティ株式会社 e-Gate センター

続報：Apache Log4j の脆弱性情報について

1. 概要

2021 年 12 月に、Java のログ出力ライブラリー「Apache Log4j」の深刻な脆弱性（CVE-2021-44228）が報告されました。

開発者からこの脆弱性に対する修正版が公開された後も、複数の新たな脆弱性（CVE-2021-45046，CVE-2021-45105，CVE-2021-44832）が発覚しました。これらの「Apache Log4j」に関する脆弱性は通称「Log4jShell」と呼ばれています。

「Apache Log4j」は Java のログ出力用オープンソースソフトウェアとして幅広く用いられているため、影響を受ける可能性のあるシステムは大量に存在します。また、米国ではCISAが「Log4jShell」への対処を命じる緊急指令を発令しており、世界的に今後の影響が注目されています。

今回は新たに公開されたこれらの「Apache Log4j」の脆弱性と最新の動向についてご紹介いたします。

※CVE：共通脆弱性識別子。個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体の MITRE 社が主要な脆弱性情報サイトと連携して採番している識別子です。

※CISA：米国サイバーセキュリティ・インフラストラクチャセキュリティ庁。米国国土安全保障省に属する政府機関であり、情報セキュリティとインフラの安全に関わる業務を行っています。

2. 最近公開された Apache Log4j の脆弱性情報

12 月 10 日に CVE-2021-44228 が公表されて以来、現在までに「Apache Log4j」（以降は Log4j と記載）の脆弱性として以下の４つが報告されています。

(1) CVE-2021-44228

Log4j の JNDI（Java Name and Directory Interface）の Lookup 機能に関する脆弱性で、悪用された場合、遠隔の第三者が細工した文字列を送信し、Log4j がログとして記録することで任意のコードを実行される可能性があります。

Lookup 機能の悪用による攻撃についての詳細は以下の過去に取り上げたセキュリティニュースをご参照ください。
『注意喚起：Apache Log4j の脆弱性情報について』（2021 年 12 月）
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=12180

(2) CVE-2021-45046

バージョン 2.15.0 での修正不十分を原因とし、特定の構成においてサービス運用妨害が生じる脆弱性と報告されましたが、のちに任意のコードを実行される脆弱性に修正されました。

(3) CVE-2021-45105

再帰的 Lookup を行う特定の設定において、サービス運用妨害が行われる脆弱性です。

(4) CVE-2021-44832

ログ設定ファイルを変更する権限を持つ攻撃者により任意のコードを実行される脆弱性です。

影響を受けるバージョン等についての情報は表 1 のとおりです。

CVE-ID	影響を受けるバージョン	修正版			CVSSv3
		Java 8 以降	Java 7	Java 6	
CVE-2021-44228	Log4j 2.0-beta9 から 2.14.1	Log4j 2.15.0	Log4j 2.12.2	Log4j 2.3.1	10.0
CVE-2021-45046	Log4j 2.0-beta9 から 2.15.0 (2.12.2 を除く)	Log4j 2.16.0			9.0
CVE-2021-45105	Log4j 2.0-beta9 から 2.16.0 (2.12.3 を除く)	Log4j 2.17.0	Log4j 2.12.3		5.9
CVE-2021-44832	Log4j 2.0-alpha7 から 2.17.0 (2.3.2、2.12.4 を除く)	Log4j 2.17.1	Log4j 2.12.4	Log4j 2.3.2	6.6

【表 1】Log4j 関連の脆弱性情報

※CVSSv3：共通脆弱性評価システムといい、基本評価基準・現状評価基準・環境評価基準の 3 つの基準で IT 製品のセキュリティ脆弱性の深刻さを評価した値です。情報システムの脆弱性に対するオープンで汎用的な評価手法で、0.0～10.0 の範囲（値が大きいほど深刻）で深刻度をスコア化しています。

3. Apache Log4j 関連の脆弱性対策

国内外で本脆弱性に対する攻撃を検知していることが発表されており、影響を受けるバージョンの Log4j を利用している場合速やかに対応する必要があります。

一連の Log4j 脆弱性に対しては以下の対策が有効です。その他、システムから外部への接続を制限するアクセス制御の強化なども軽減策として効果的です。

(A) 最新アップデートの適用

The Apache Software Foundation から本脆弱性を修正した以下のバージョンが提供されています。これらの修正済みバージョンでは Log4j の Lookup 機能がデフォルトで無効化されています。

- Log4j 2.17.1（Java 8 以降向け）
- Log4j 2.12.4（Java 7 向け）
- Log4j 2.3.2 （Java 6 向け）

(B) 回避策の実行

最新アップデートがすぐに適用できない場合の回避策として、特定の class ファイル（Jndilookup.class）をクラスパスから削除する方法が有効です。

なお、「2.最近公開された Apache Log4j の脆弱性情報」で取り上げた過去セキュリティニュース『注意喚起：Apache Log4j の脆弱性情報について』記載の「Lookup 機能の無効化」及び「PatternLayout の変更」については CVE-2021-45046 に対して有効ではないためご注意ください。

4. Apache Log4j 脆弱性の最新の動向

下記表 2 に Log4j 脆弱性についてのタイムラインをまとめています。

過去最悪クラスと評され次々と脆弱性の情報が公開された Log4j 脆弱性の残した爪痕は大きく、セキュリティ対策組織も大々的に注意を促しており、2022 年に入ってもその危険性に注目が向けられています。

【表 2】Log4j 脆弱性関連タイムライン

2021/11/25	Alibaba Cloud Security Team が The Apache Software Foundation へ脆弱性報告
2021/12/10	Twitter (@p0rz9)にて JNDI Lookup 機能を悪用した任意のコード実行に関する実証(PoC)コードが公開(現在はツイート削除済み)
〃	CVE-2021-44228 の脆弱性情報公開
〃	CVE-2021-44228 に対するセキュリティパッチ Log4j 2.15.0 リリース
2021/12/11	CVE-2021-44228 を悪用する PoC コードが公開され、国内にて本脆弱性の悪用を試みる通信が多数確認される
2021/12/15	CVE-2021-45046 の脆弱性情報公開
〃	CVE-2021-45046 に対するセキュリティパッチ Log4j 2.16.0 及び 2.12.2 (Java7 向け) リリース
2021/12/18	CVE-2021-45046 に関する CVSS が再評価され、任意のコード実行が可能であるとして情報が修正される
2021/12/19	CVE-2021-45105 の脆弱性情報公開
〃	CVE-2021-45105 に対するセキュリティパッチ Log4j 2.17.0 リリース
2021/12/22	CVE-2021-44228, CVE-2021-45046, CVE-2021-45105 に対するセキュリティパッチ Log4j 2.12.3 (Java7 向け) 及び 2.3.1 (Java6 向け) リリース
2021/12/28	CVE-2021-44832 の脆弱性情報公開
〃	CVE-2021-44832 に対するセキュリティパッチ Log4j 2.17.1 、Log4j 2.12.4 (Java7 向け) 及び 2.3.2 (Java6 向け)リリース
2022/1/4	米国連邦取引委員会、Log4j 脆弱性への対策を行わない企業に法的措置を講じる可能性があると表明
2022/1/14	Google、Log4j 脆弱性を受けオープンソースソフトウェアの管理を支援する組織の設立を提案

5. 攻撃による被害

現在までに確認されている Log4j 脆弱性による被害として、

・仮想通貨のマイニングに利用される

・ボットネットの感染

・ランサムウェアの感染

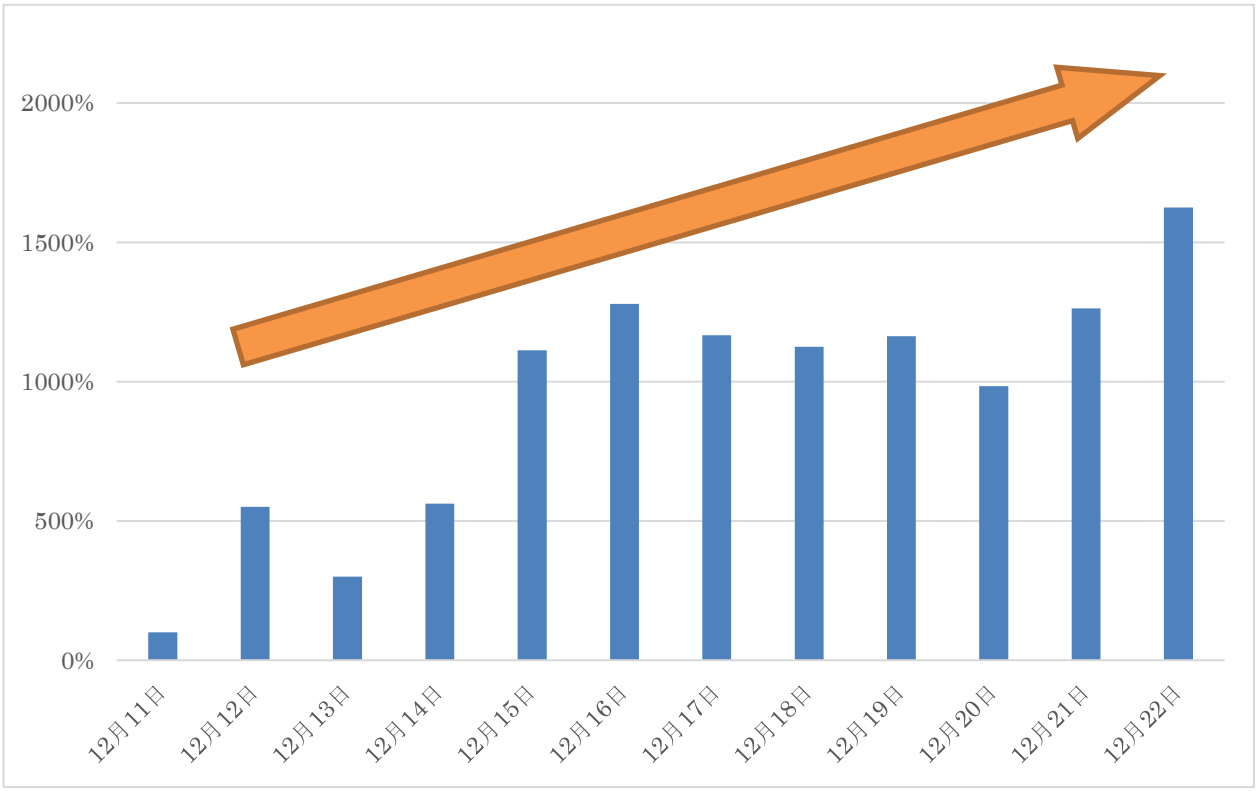
・認証情報の窃取

などが報告されています。

また、Microsoft 社によると Log4j 脆弱性を悪用したランサムウェア「Night Sky」により仮想デスクトップ＆アプリケーションソフトウェア「VMware Horizon」を標的とした攻撃が確認されているほか、国内企業でも同じく「Night Sky」ランサムウェア被害に遭うなどの実例が確認されています。

6. e-Gate センターにおける攻撃検知の推移

e-Gate センターでも Log4j 脆弱性をついた攻撃を継続的に検知しております。下図は 12 月 10 日に CVE-2021-44228 の脆弱性情報が公開されて以降約 2 週間の検知数です。脆弱性が公開されて数日で攻撃が急増し、その後も継続的に検知されているため、引き続き注意が必要です。



【図 3】e-Gate センターにおける Log4j シグネチャ検知傾向

（12 月 11 日を 100%として算出）

7. 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
更新：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

・ITmedia
「Log4j」2.17.0 にもリモートコード実行の脆弱性　修正バージョン公開
https://www.itmedia.co.jp/news/articles/2112/29/news060.html

・Microsoft
Guidance for preventing, detecting, and hunting for exploitation of the Log4j 2 vulnerability
https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

8. 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