Log4Shellによってもたらされるサイバー脅威から お客様を保護するCrowdStrike Falcon

December 15, 2021 | Farid Hendi - Karan Sood - Liviu Arsene | エンドポイントとクラウドセキュリティ

- Log4j2 Apache Logging Servicesライブラリにある最新の重大な脆弱性であるLog4Shellは、組織に深刻な脅威をもたらします。
- 脆弱性を悪用する積極的な試みが実際に確認されており、現在最も深刻な脅威となっています。
- CrowdStrikeは、攻撃の痕跡（IOA: Indicators of Attack）と機械学習を利用して、お客様を保護します。
- CrowdStrikeは、Log4Shellの進化を追跡および監視し続け、お客様を保護するために必要な対策を更新および展開します。
- Log4j2を使用している組織は、ライブラリを2021年12月14日に公開された最新のLog4j2（2.16.0）バージョンに更新することを強くお勧めします。
- CrowdStrike Falconの展開において、エージェントの更新や緩和策などは必要ありません。詳細については**Knowledge Base**をご確認ください。

Log4Shell（**CVE-2021-44228**, **CVE-2021-45046**）の脆弱性に関する**最近の CrowdStrike Intelligence チームの調査結果**は、広範囲にわたる影響を示しています。 CrowdStrike は、機械学習と攻撃の痕跡（IOA）の両方を使用し、この脆弱性を利用し行われる脅威からお客様を保護します。

Log4Shell は、一般的な Java ライブラリの脆弱性であり、オンラインゲームからクラウドインフラストラクチャまであらゆる場所で見うけられます。 脆弱性を悪用する積極的かつ継続的な試みが CrowdStrikeFalconOverWatch™ によって確認されています。 経済的に動機付けられた攻撃者グループは、すぐに公開されている概念実証（POC）コードを採用し、脆弱なターゲットシステムに悪意のあるペイロードを展開しています。ほとんどの展開されたペイロードには、XMRig マイナー、リバースシェル、リモートアクセストロイの木馬、ボットネットが含まれます。

CrowdStrike はさまざまなメカニズムを使用して、Log4j2 の脆弱性を悪用するペイロードからお客様を保護します。 CrowdStrike Falcon の機械学習と IOA は、CVE-2021-44228 の開示以来、エクスプロイト後の活動を防御してきました。

CrowdStrike は、引き続き Log4Shell の進化を積極的に監視し、Log4j2 の脆弱性の結果として、エクスプロイト後のアクティビティからお客様を保護するために必要な対策を展開します。

脆弱性の影響と悪用

Log4j2 はオープンソースライブラリである Apache Logging Services の一部であり、Java で記述されており、Elasticsearch、Flink、Kafka などのさまざまなフレームワークで使用されます。 Java はクロスプラットフォームフレームワークであるため、Log4j2 の脆弱性は特定のオペレーティングシステムで実行されているアプリケーションに限定されません。

適切な緩和策やパッチを適用しないと、攻撃者はこの脆弱性を利用して、システムにマルウェア、リバースシェル、その他の脅威を展開する可能性があります。

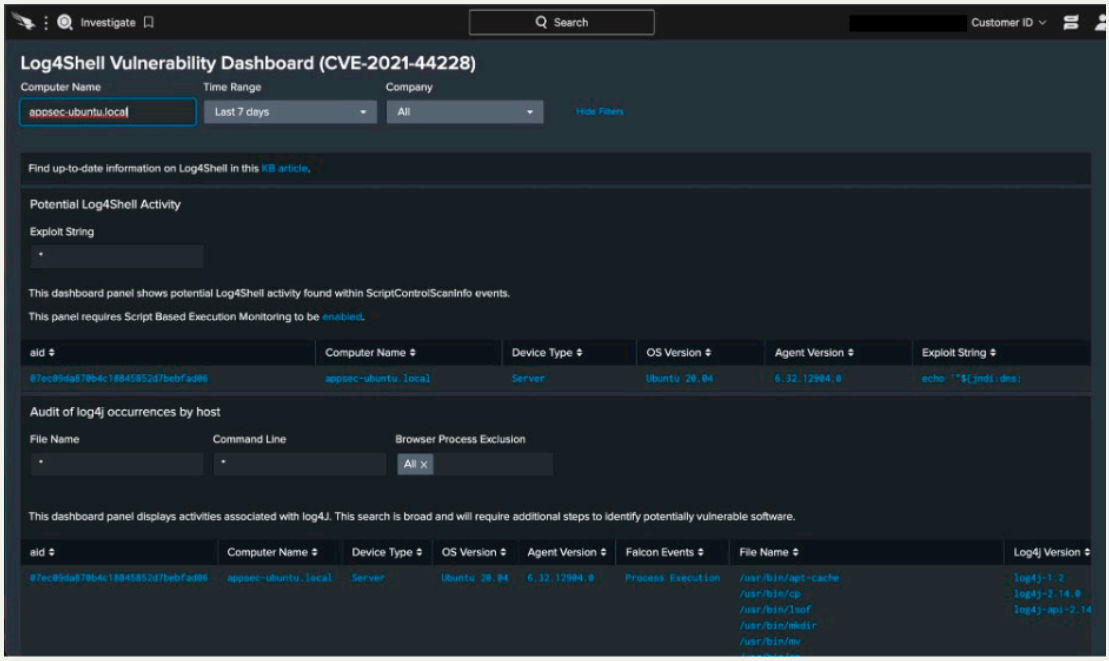
CrowdStrike Intelligence によると、攻撃者は、オペレーティングシステムに関係なく、脆弱なシステムやサービスを標的にしたアクティブなスキャンと悪用の試みを開始しました。

Linux はクラウドインフラストラクチャで重要な役割を果たしているため、Log4j2 の脆弱性を使用して展開されたペイロードに関するレポートでは、脆弱性が公開されてから数日後に、Mirai や Muhstik などのボットネットがデバイスを標的にし始めたことが明らかになりました。

Log4j2 の悪用に対して脆弱なオペレーティングシステムとフレームワークを標的とする他の脅威に関する業界レポートには、ターゲット環境に足場を確立するために展開されているビーコン（Cobalt Strike や Metasploit など）が含まれます。

Falcon のお客様が Log4j2 を探す方法

モジュール Log4j2 は、数多くのサードパーティソフトウェアパッケージにバンドルされています。 このため、Log4j2 の存在を探すことは、その実行可能ファイル、SHA256、またはファイルパスを探すことほど簡単ではありません。 CrowdStrike Falcon のお客様には、ダッシュボードを構築して提供しております。こちらを利用し、サポートされているすべてのオペレーティングシステム環境における Log4j2 の脆弱性の積極的な悪用を特定できます。



（クリックして拡大表示）

ダッシュボードに加えて、お客様は Falcon センサーからのテレメトリを使用して、開発者がアプリケーションで使用する方法と合わせて、Log4j2 の利用状況を確認できます。 Log4j2 の使用状況を検索するための Falcon Insight™ クエリは次のとおりです：

```
event_simpleName IN（ProcessRollup2, SyntheticProcessRollup2, JarFileWritten, NewExecutableWritten, PeFileWritten, ElfFileWritten）
| search *log4j*
| eval falconEvents=case（event_simpleName="ProcessRollup2", "Process Execution", event_simpleName="SyntheticProcessRollup2", "Process Execution", event_simpleName="JarFileWritten", "JAR File Write", event_simpleName="NewExecutableWritten", "EXE File Write", event_simpleName="PeFileWritten", "EXE File Write", event_simpleName=ElfFileWritten, "ELF File Write"）
| fillnull value="-"
| stats dc（falconEvents）as totalEvents, values（falconEvents）as falconEvents, values（ImageFileName）as fileName, values（CommandLine）as cmdLine by aid, ProductType
| eval productType=case（ProductType = "1","Workstation", ProductType = "2","Domain Controller", ProductType = "3","Server", event_platform = "Mac", "Workstation"）
| lookup local=true aid_master aid OUTPUT Version, ComputerName, AgentVersion
| table aid, ComputerName, productType, Version, AgentVersion, totalEvents, falconEvents, fileName, cmdLine
| sort +productType, +ComputerName
```

Log4j2 の悪用の試みを探すためのクエリは次のとおりです：

```
search index=main event_simpleName=Script* cid=* ComputerName=*
| eval ExploitStringPresent = if（match（ScriptContent,"（env|jndi|ldap|rmi|ldaps|dns|corba|iiop|nis|nds）"）,1,0）
| search ExploitStringPresent = 1
| rex field=ScriptContent "（?i）（?<ExploitString>.*j'?\}?（?:\$\{[^}]+:['-]?）?n'?\}?（?:\$\{[^}]+:['-]?）?d'?\}?（?:\$\{[^}]+:['-]?）?i'?\}?（?:\$\{[^}]+:['-]?）?:'?\}?[^/]+）"
| eval HostType=case（ProductType = "1","Workstation", ProductType = "2","Domain Controller", ProductType = "3","Server", event_platform = "Mac", "Workstation"）
| stats count by aid, ComputerName, HostType, ExploitString
| lookup local=true aid_master aid OUTPUT Version, ComputerName, AgentVersion
| table aid, ComputerName, HostType, Version, AgentVersion ExploitString
| rename ComputerName as "Computer Name", HostType as "Device Type", Version as "OS Version", AgentVersion as "Agent Version", ExploitString as "Exploit String"
| search "Exploit String"="***"
```

CrowdStrike は、機械学習と IOA（攻撃の痕跡）を使用して保護

CrowdStrike Falcon の緩和策は、使用される特定のエクスプロイトではなく、攻撃者やテスターが使用する戦術や手法を対象としています。CrowdStrike Falcon は、機械学習と IOA を活用して、エンドポイント上の悪意のあるプロセスまたはスクリプトの動作をターゲットとすることで、悪意のある脅威に対してさまざまな角度からカバレッジを提供します。

機械学習がもたらす独自の利点は、ファイルの属性に基づいて悪意を理解することにより、既知と未知両方のマルウェアまたは脅威を識別できることです。 CrowdStrike Falcon センサーは、Windows、Linux、および macOS プラットフォームで、エンドポイント上のセンサー内とクラウド内の両所で機械学習を活用して、攻撃者によって現在展開されている Log4j2 の脆弱性を利用した脅威を検知および防御します。ランサムウェア、暗号通貨マイニング、トロイの木馬、ボットネットなどのマルウェアファミリーなどさまざまな防御に非常に効果的です。

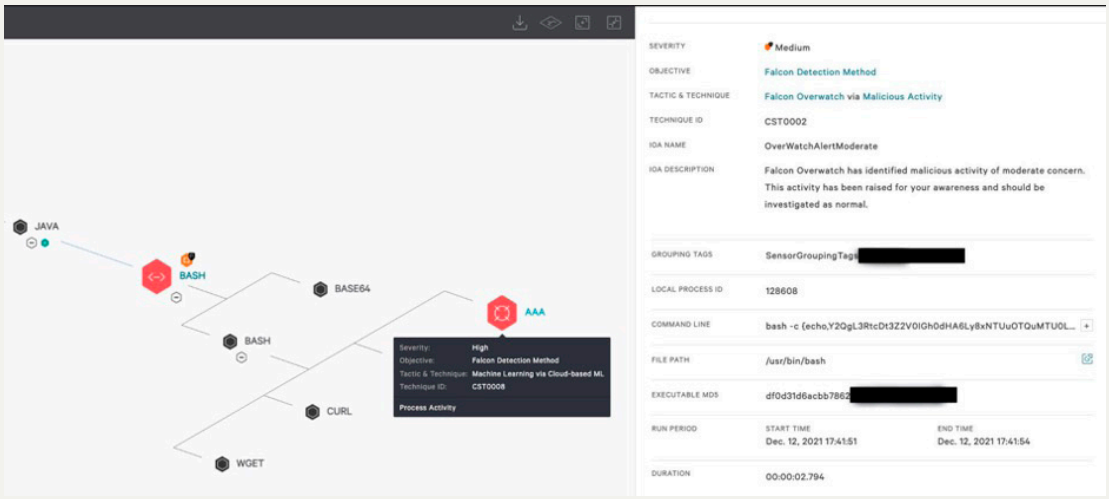


図 1. 悪意のある Bash プロセスに関する Falcon OverWatch からの通知と、後続のダウンロードされたペイロードでの ML 検知を表示するスクリーンショット（クリックして拡大）

図 1 は、Log4j2 の脆弱性が悪用された結果、成功したエクスプロイトのその後のアクティビティを示しています。 ご覧のとおり、Java での bash プロセスが、wget および cURL ユーティリティを利用して、AAA で示される第 1 段階のペイロードをダウンロードしました。これは、Falcon のセンサー上の機械学習モデルによってブロックされています。注目すべきことは、Falcon の機械学習は、Log4j2 の脆弱性が発表される前から、エクスプロイト後のアクティビティをプロアクティブにカバーしていました。

機械学習での防御に加えて、スクリーンショットには、Falcon OverWatch チームが Java での悪意のある bash プロセスを検出してアラートを出しています。CrowdStrike がお客様を保護するために使用する多層アプローチを例示しています。

Log4j2 の脆弱性を悪用する攻撃者によって最近展開された脅威を含め、脅威の検知に関して Falcon が採用する戦略の重要な部分が、IAO です。 このアプローチは、攻撃で明示的に使用されたマルウェアに関係なく、攻撃者が達成しようとしている振る舞いを検知することに重点を置いています。

たとえば、CrowdStrike Falcon センサーは、**既存**の IOA を使用して、展開された複数の脅威を防御することができました。CrowdStrike Falcon は、攻撃者が実行しようとする一連の動作と戦術にフォーカスして観察することにより、同様の振る舞いを示す新しい未知の脅威を正常に検知してブロックすることができます。

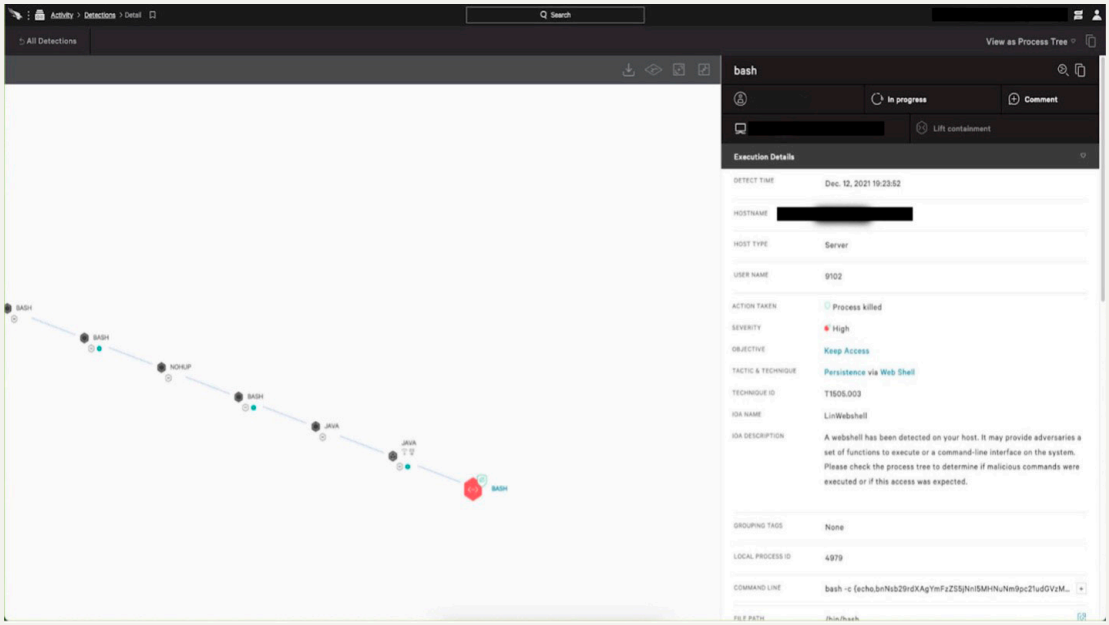


図 2.Falcon IOA が Log4j2 のエクスプロイト後の悪意のあるアクティビティを防御していることを示す画面ショット（クリックして拡大）

図 2 は、プロセスがペイロードをダウンロードする前に、Falcon IOA が同じ悪意のあるアクティビティを防御、強制終了したことを示しています。 この防御の結果として、エンドポイントでその後の悪意のあるエクスプロイト後のアクティビティは発生しませんでした。 IOA は動的に展開され、センサーの更新は必要ありません。CrowdStrike Content Research & Response チームは、脆弱性の開示から数時間以内に 20 を超える新しい IOA をリリースし、Log4j2 の悪用後のアクティビティに対する Falcon の検知範囲を強化することができました。

Windows、Linux、macOS のいずれであっても、CrowdStrike Falcon センサーは、振る舞い検知、機械学習、高度なエクスプロイト防御の機能を活用して、お客様を保護し、**侵害を阻止**します。

推奨事項

- Log4j2を使用している組織は、ライブラリを最新のバージョンに更新することを強くお勧めします。
- インフラストラクチャ全体、ソフトウェアアプリケーション、およびソフトウェアサプライチェーンを監査して、ApacheLog4j2ロギングフレームワークへの依存関係を確認してください。
- CrowdStrikeFalconのお客様は、Preventionポリシーが**ベストプラクティス**に従っているかを確認してください。
- 重要なアプリケーション/サービスを特定し、状況が進展してもベンダー固有の推奨事項を最新の状態に保つ様努めてください。

Note: CrowdStrike Falcon のお客様は、Log4j2 / Log4Shell に対して脆弱なシステムを特定しリスクを軽減する詳細な手順を、**Support Portal** でご確認いただけます。

関連情報

- Log4Shell 脆弱性に関して CrowdStrike Intelligenceチームのブログで紹介しています
- 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：How CrowdStrike Protects Customers from Threats Delivered via Log4Shell
https://www.crowdstrike.com/blog/how-crowdstrike-protects-customers-from-log4shell-threats/