2022.01.06

【重要】Log4j の脆弱性が NX に与える影響と対策について

＜影響＞

Java のロギングライブラリ「Apache Log4j」で任意のコード実行が可能になる脆弱性（CVE-2021-44228）が報告されています。
本脆弱性を悪用した攻撃が行われる可能性に対応するため至急、下記の＜対策＞および＜対応方法＞を実施してください。

※本件脆弱性への対応につきまして、検索対象の.jar ファイルの追加(TCInterface.jar)と、外部プログラムを使用した対応方法を追加します。
何れかの方法にて、対策をお願いいたします。

＜影響のある NX バージョン＞

すべてのリリース

＜脆弱性が確認されている Log4j のバージョン＞

Log4j 2.0～2.14.0

＜対策＞

classpath から特定の class ファイル（JndiLookup.class）を削除します。

＜対応方法 1 ＞

■手動による検索と削除

●対象ファイルの検索

問題を引き起こす jar ファイル（log4j-core-<version>.jar、TCInterface.jar）が端末内に含まれていないかを検索して下さい。

＊ Windows のフォルダ内検索を使用する場合は、「log4j-core-2」「TCInterface.jar」で検索してください。
＊「NX インストールフォルダ¥UGMANAGER¥tccs¥third_party¥TcSS¥TcSSxx.x¥jars¥log4j-core-2.x.x.jar」ファイルなどが該当します。
＊「log4j-core-2.x.x.jar」「TCInterface.jar」ファイルがない場合は、影響ありません。

●削除

jar ファイルを修正する必要があります。
ここでは「7 -Zip」というアプリケーションを用いた手順を一例として記載いたします。
ご利用の環境にあわせて修正を実施してください。

1. 検索で見つかったファイルが読み取り専用の場合は、属性を解除します（マウス右ボタン→プロパティ）。
2. 検索で見つかったファイルをコピーしてバックアップを取ります(拡張子を変えます)。
   例：log4j-core-2.13.0.jar → log4j-core-2.13.0.jar_copy

3. log4j-core-2.13.0.jar ファイルを右クリックし、「7-Zip」→「開く」を選択します。

4. 以下のフォルダまで展開します。
org/apache/logging/log4j/core/lookup

5. 以下のファイルを削除します。
JndiLookup.class

6. ファイルの読み取り専用の属性を元に戻します（マウス右ボタン→プロパティ）

7. 見つかったすべての対象ファイルについて、手順 1～6 を繰り返し実行します。

＜対応方法２＞
■外部ツールを利用した検索と削除

1. 下記のリンク先より「log4j2-scan 2.5.3 (Windows x64, zip)」をダウンロードします。

Log4j2-scan by Logpresso
https://github.com/logpresso/CVE-2021-44228-Scanner

   ＊本ツールは、本問題への対応として SIEMENS 社から推奨されているツールとなります。

2. ダウンロードしたファイルを解凍します（log4j2-scan.exe ファイルが解凍先フォルダ内にあります）。
3. コマンドプロンプトにて、以下のコマンドを実行します。

   log4j2-scan.exe --fix <NX インストールフォルダのフルパス>

※本コマンドを実行すると自動的に処理対象となった XXX.jar が、
      log4j2_scan_backup_xxx_xxx.zip ファイル内にバックアップされます

4. 以下のように修正されたファイルがコマンドプロンプト上にリストされます。
   ：
   Fixed: C:¥Siemens¥NX1926¥UGMANAGER¥soa¥tc12000.4.0¥log4j-core-2.13.0.jar
   Fixed: C:¥Siemens¥NX1926¥UGMANAGER¥tccs¥third_party¥TcSS¥TcSS12.4¥jars¥log4j-core-2.13.0.jar
   Fixed: C:¥Siemens¥NX1926¥DESIGN_TOOLS¥checkmate¥tools¥quality_dashboard¥TCInterface.jar
   ：

5. 以上で処理は完了していますが、確認のためコマンドプロンプトにて以下のコマンドを実行します。

   log4j2-scan.exe --report-csv <NX インストールフォルダのフルパス>

6. コマンドプロンプトのカレントディレクトリに、log4j2_scan_report_xxx_xxx.csv ファイルが出力されます。
7. csv ファイルを Excel で開きます。
   対象となった jar ファイル等のリストと Status を確認できます。
   Status が"MITIGATED"となっているファイルが対処済のファイルです。

   ※ SIEMENS 社 参照 SFB:PL8600959
   ※ ご不明な点がございましたら弊社まで、または ISID Customer Center へお問い合わせください。

以上