【重要】Log4j の脆弱性が Siemens Help Server に与える影響と対策について (NX1926 以降)

＜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。

＜影響のある Siemens Documentation Server バージョン＞

Siemens Documentation Server 1.0.x
Siemens Documentation Server 2.0.x

※NX1926 シリーズ以降に対応した Help Server をインストールされたお客様が対象となります。
Windows コントロールパネルの「プログラムと機能」では、"Siemens ヘルプサーバ"と表示されます。

※Help Server のバージョンは、インストールフォルダ（通常は C:¥Program Files¥Siemens¥HelpServer）内の ～¥logs¥app.log に記述があります。

＜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＞

Siemens Documentation Server 1.0.x をインストールされている場合は、2.0.x へアップグレードし、次項の対策を実施します。
（アップグレードには、2.0.x のインストーラ(HelpServer.2.0.0.exe)を Siemens Support Center Web よりダウンロードして実行します。）

Siemens Documentation Server 2.0.x では、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）がインストールフォルダ内に含まれていないかを検索してください。

＊ Windows のフォルダ内検索を使用する場合は、「log4j-core-2」で検索してください。
＊ 「C:¥Siemens¥Help Server¥elasticsearch-6.6.2¥lib¥log4j-core-2.11.1.jar」ファイルが該当します。

●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. サービスの停止
   Windows のタスクマネージャから[サービス」タブへ移動し、下記サービスをマウス右ボタンでクリックし、[停止]を選択します。
   Elasticsearch 6.6.2-SNAPSHOT(SiemensPLMElasticSearchServer)

2. 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）。

3. 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-2.11.0.jar → log4j-core-2.11.0.jar_copy

4. log4j-core-2.11.0.jar ファイルを右クリックし、「7-Zip」→「開く」を選択します。

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

6. 以下を削除します。
   JndiLookup.class

7. 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）。

8. サービスの起動
   Windows のタスクマネージャから[サービス」タブへ移動し、下記サービスをマウス右ボタンでクリックし、[開始]を選択します。
   Elasticsearch 6.6.2-SNAPSHOT(SiemensPLMElasticSearchServer)

＜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 2.7.2 (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. サービスの停止
Windows のタスクマネージャから[サービス」タブへ移動し、下記サービスをマウス右ボタンでクリックし、[停止]を選択します。
Elasticsearch 6.6.2-SNAPSHOT(SiemensPLMElasticSearchServer)

4. 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 <Help 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。

5. 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:¥Program Files¥Siemens¥HelpServer¥elasticsearch-6.6.2¥lib¥log4j-core-2.11.1.jar
:

6. 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 <Help インストールフォルダのフルパス>

7. 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。

8. 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。

9. サービスの起動
Windows のタスクマネージャから[サービス」タブへ移動し、下記サービスをマウス右ボタンでクリックし、[開始]を選択します。
Elasticsearch 6.6.2-SNAPSHOT(SiemensPLMElasticSearchServer)

※ SIEMENS 社 参照 SFB:PL8601245

※ 次の Siemens Documentation Server 2.1 リリースでは、脆弱性を含まないように修正予定です。

※ SIEMENS 社より追加の情報が入り次第、本情報も更新いたします。

※ ご不明な点がございましたら弊社、または ISID Customer Center までお問い合わせください。

以上