【重要】Log4j の脆弱性が Siemens Documentation Server に与える影響と対策について (NX10～NX1899 シリーズ)

＜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 4.2.1

※NX10～NX1899 シリーズに対応した Documentation Server をインストールされたお客様で、
上記バージョンのみが対象となります。
Windows コントロールパネルの「プログラムと機能」では、"Siemens PLM Documentation Server" と表示されます。

＜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＞

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

＜対応方法＞

●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:¥Program Files¥Siemens¥PLM Documentation Server¥SolrServer¥lib¥ext¥
log4j-core-2.11.0.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。
   ・Siemens PLM Solr Server
   ・Siemens PLM Documentation Server

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。
   ・Siemens PLM Solr Server
   ・Siemens PLM Documentation Server

※ SIEMENS 社 参照 SFB:PL8601245
※ 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