2021 年 11 月 22 日

お客様各位

株式会社　セゾン情報システムズ
カスタマーサービスセンター

DataSpider BPM 製品における Apache Tomcat の脆弱性（CVE-2021-41079）に対する報告

DataSpider BPM 製品における Apache Tomcat の脆弱性(CVE-2021-41079）に対する報告をご案内いたします。

\- 記 -

1. 脆弱性の内容

- CVE-2021-41079
  Apache Tomcat が TLS 用に NIO+OpenSSL または NIO2+OpenSSL で構成されている場合、特別に細工されたパケットを使用することで無限ループが発生し DoS を引き起こすことができる可能性があります。

2. 調査状況

DataSpider BPM 2.6 では NIO+OpenSSL を使用しているため、本脆弱性の対象環境に該当します。

3. 対象製品

影響を受ける対象の DataSpider BPM バージョンは以下の通りです。

- DataSpider BPM 2.6
  ※2.5 以前のバージョンは、対象外となります。

4. 対応方法

- 以下の対応により、NIO と OpenSSL を使用しない状態となります（脆弱性の影響を受けません）。

1. DataSpider BPM サーバを停止します。
   サーバの停止に関する詳細は、インストールガイド (DataSpiderBPM26_InstallGuide.pdf) の「4.2. 停止」を参照してください。

2. server.xml ファイルを開きます。
   [場所]：<DataSpider BPM インストールディレクトリ>¥conf¥server.xml

3. server.xml を修正します。
   以下の記載内容をコメントアウトします。
   <Listener className="org.apache.catalina.core.AprLifecycleListener"
   SSLEngine="on" />

   修正例）
   <!--
   <Listener className="org.apache.catalina.core.AprLifecycleListener"
   SSLEngine="on" />
   -->

4. server.xml を保存して閉じます。

5. tcnative-1.dll ファイルを別のディレクトリに適宜バックアップします。
   [場所]：<DataSpider BPM インストールディレクトリ>¥apache-tomcat¥bin¥tcnative-1.dll

6. tcnative-1.dll ファイルを削除します。

7. DataSpider BPM サーバを起動します。
   サーバの起動に関する詳細は、インストールガイド(DataSpiderBPM26_InstallGuide.pdf) の「4.1. 起動」を参照してください。

設定が適用されているかは以下の手順で確認が可能です。

1. DataSpider BPM サーバを起動後、catalina.log ファイルを開きます。
   [場所]：<DataSpider BPM インストールディレクトリ>¥logs¥catalina.<yyyy-mm-dd>.log

2. catalina.log ファイルの内容を確認します。

・以下のログが出力されていないことを確認してください。

情報 [main] org.apache.catalina.core.AprLifecycleListener.lifecycleEvent APR バージョン[1.7.0]を使用して APR ベースの Apache Tomcat ネイティブライブラリ[1.2.23]をロードしました。

・以下のログが出力されていることを確認してください。

-SSL 設定を行っていない場合

情報 [main] org.apache.coyote.AbstractProtocol.start プロトコルハンドラー ["http-nio-18080"] を開始しました。

※「18080」は、SSL 設定を行っていない場合のデフォルトのポート番号となります。
　ポート番号を変更している場合は適宜読み替えてください。

-SSL 設定を行っている場合

情報 [main] org.apache.coyote.AbstractProtocol.start プロトコルハンドラー ["https-jsse-nio-18443"] を開始しました。

※「18443」は、SSL 設定を行っている場合のデフォルトのポート番号となります。
ポート番号を変更している場合は適宜読み替えてください。

※今回の脆弱性は OpenSSL に関連したものとなりますが、OpenSSL に関してはこれまでにも複数の脆弱性が報告されております。本対応により OpenSSL を使用しない状態となりますため、今回の脆弱性のリスクを許容可能な場合にも、本対応の実施を推奨いたします。

以上

【改訂履歴】

2021 年 11 月 22 日	初版作成