2020 年 3 月 16 日

お客様各位

株式会社セゾン情報システムズ
HULFT 事業部

DataSpider BPM 製品における Apache Tomcat の脆弱性

(CVE-2020-1938、CVE-2020-1935）に対する報告

DataSpider BPM 製品における Apache Tomcat の脆弱性(CVE-2020-1938、CVE-2020-1935）に対する報告をご案内いたします。

- 記 -

1. 脆弱性の内容

- CVE-2020-1938
  Apache JServ Protocol (AJP) 通信において、AJP リクエストインジェクションとリモートコード実行ができてしまう脆弱性となります。

- CVE-2020-1935
  HTTP ヘッダの行末の判定処理に問題があり、不正な HTTP ヘッダが送られてもサーバが正常に処理しようとする脆弱性となります。

2. 調査状況

- CVE-2020-1938
  AJP プロトコル通信を使用していませんが、AJP プロトコル通信（ポート: 18009）を有効な状態にしているため、影響を受ける可能性があります。

- CVE-2020-1935
  影響度が「低」となっており、不正な HTTP ヘッダが送られても、リモートコードの実行などは行われないため、本脆弱性だけでの影響は低いと判断しております。

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 2.5
- DataSpider BPM 2.4
- DataSpider BPM 2.3

4. 回避方法

- CVE-2020-1938 については、以下の対応にて回避可能となります。

  $DSBPM_HOME¥conf¥server.xml の以下の設定を削除またはコメント化してください。
  「protocol="AJP/1.3"」の記載がある <Connector> タグ

  ```
  <Connector port="18009" protocol="AJP/1.3"
  redirectPort="18443"
  useBodyEncodingForURI="true" />
  ```

※ 上記設定変更を有効にするため、DataSpider BPM のサービス再起動が必要となります。

5. 今後の対応

DataSpider BPM 2.6 (7 月リリース予定)にて対応予定です。

以上

【改訂履歴】

2020 年 3 月 16 日	初版作成