

お客様各位

株式会社セゾン情報システムズ

HULFT 事業部

HULFT Series 製品における Tomcat の脆弱性 (CVE-2017-5664) に対する報告

HULFT Series 製品における Tomcat の脆弱性 (CVE-2017-5664) に対する報告をご案内いたします。

- 記 -

## 1. 脆弱性の内容

Tomcat において、脆弱性が公表されました (CVE-2017-5664)。細工された HTTP リクエストを処理することで、エラーページの削除や上書きが行われる可能性があります。

< Tomcat の脆弱性に関する情報 >

▼JVNVU#95420726 Apache Tomcat にセキュリティ制限回避の脆弱性

<http://jvn.jp/vu/JVNVU95420726/index.html>

▼Learn more at National Vulnerability Database

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638>

## 2. 調査状況

上記脆弱性について HULFT Series 製品における影響をご案内いたします。

<HULFT Series 製品 調査状況 - 2017年6月14日 9:00時点>

製品名	調査状況
HULFT	影響ありません。
HULFT BB	影響ありません。
HULFT8 Script Option	影響ありません。
HULFT IoT	影響ありません。
HULFT-HUB	影響ありません。
HULFT-DataMagic (Ver. 1, 2) DataMagic (Ver. 3)	影響ありません。
HULFT クラウド (Ver. 1) HULFT-WebFT (Ver. 2) HULFT-WebFileTransfer (Ver. 3)	影響ありません。
HULFT-WebConnect	影響ありません。
HDC-EDI Suite	<HDC-EDI Base> 影響を受けます。 ご利用の HDC-EDI Base が対応している最新の Tomcat へ アップデートしてください。

	<p>&lt;HDC-EDI Manager &gt; 影響を受けます。 ご利用の HDC-EDI Manager が対応している以下の Tomcat へアップデートしてください。</p> <ul style="list-style-type: none"> <li>・Apache Tomcat 8.5.15</li> <li>・Apache Tomcat 8.0.44</li> <li>・Apache Tomcat 7.0.78</li> </ul> <p>ただし、Apache Tomcat 8.5.15 を利用する場合は 暫定対応として下記の作業が必要となり、かつ制限事項があります。</p> <p>[作業] 下記のファイルをテキストエディタで開き、1行目の charset の値を Shift-JIS へ変更してください。</p> <ul style="list-style-type: none"> <li>・Tomcat のインストールディレクトリ/appBase ディレクトリ/hdcweb/WEB-INF/views/suggest.jsp</li> <li>・Tomcat のインストールディレクトリ/appBase ディレクトリ/hdcweb/WEB-INF/views/include/renkeihistory/hdc_lgl111_historyframe_v2.jsp</li> </ul> <p>appBase ディレクトリは、通常「webapps」です。</p>
	<pre>&lt;%@ page contentType="text/html; charset=Shift-JIS"%&gt; &lt;%@ taglib prefix="c" uri="http://java.sun.com/jsp/jstl/core"%&gt; &lt;c:out value="\${suggestActionForm.suggestListStr}" escapeXml="false" /&gt;</pre> <p>[制限事項] 業務セット・業務情報に IBM 拡張文字・NEC 特殊文字・NEC 選定 IBM 拡張文字の範囲の文字が指定されていると、そのサジェストの候補が文字化けします。</p> <p>上記の暫定対応・制限事項については、次期リリースで対応予定です。</p>
iDIVO	影響ありません。
SIGNAIert	影響ありません。

【改訂履歴】

2017年6月15日	初版作成
------------	------

以上