

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 Java の脆弱性 (CVE-2018-2638 等) に対する報告

HULFT Series 製品における Java の脆弱性 (CVE-2018-2638 等) に対する報告をご案内いたします。

- 記 -

## 1. 脆弱性の内容

Java において、脆弱性が公表されました (CVE-2018-2638 等)。攻撃者に悪用されると、任意のコード (命令) が実行され、コンピュータを制御される可能性があります。

< Java の脆弱性に関する情報 >

▼Oracle Java の脆弱性対策について (CVE-2018-2638 等)

<https://www.ipa.go.jp/security/ciadr/vul/20180117-jre.html>

▼2018年1月 Oracle Java SE のクリティカルパッチアップデートに関する注意喚起

<https://www.jpCERT.or.jp/at/2018/at180003.html>

## 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 - 2018年1月22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	<p>下記6点の脆弱性の影響があります。</p> <p>CVE-2018-2579, CVE-2018-2582, CVE-2018-2603, CVE-2018-2618 CVE-2018-2657, CVE-2018-2663</p> <p>HULFT8 Script Option は製品同梱の Java を使用するため、お客様での update や外部 Java の使用は動作保証しておりません。HULFT8 Script Option が利用する Java の update は実施しないでください。</p> <p>今後のリリースにて修正予定です。リリース時期は未定です。決定次第、情報を更新いたします。</p>
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)	<p>下記 10 点の脆弱性の影響があります。</p> <p>CVE-2018-2579, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599 CVE-2018-2603, CVE-2018-2633, CVE-2018-2618, CVE-2018-2629 CVE-2018-2663, CVE-2018-2678</p> <p>Oracle Java をご利用のお客様は、Java の実行環境を最新に update してください。</p>
HULFT-WebConnect	<p>HULFT-WebConnect Agent/CLI において、下記 10 点の脆弱性の影響があります。</p> <p>CVE-2018-2579, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2663, CVE-2018-2678</p> <p>Oracle Java をご利用のお客様は、Java の実行環境を最新に update してください。</p>
HDC-EDI Suite	<p>HDC-EDI Base/HDC-EDI Manager において、下記 10 点の脆弱性の影響があります。</p> <p>CVE-2018-2579, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2663, CVE-2018-2678</p> <p>Oracle Java をご利用のお客様は、Java の実行環境を最新に update してください。</p>
iDIVO	影響ありません。
SIGNALert	影響ありません。

**【改訂履歴】**

2018 年 1 月 24 日	初版作成
-----------------	------

以上