2017 年 4 月 28 日

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-2017-3512）に対する報告

HULFT Series 製品における Java の脆弱性(CVE-2017-3512）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-2017-3512)。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-2017-3512 等)
https://www.ipa.go.jp/security/ciadr/vul/20170419-jre.html
▼National Vulnerability Database
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3512

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 4 月 26 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＞ クライアントおよびサーバサイドにおいて、下記 15 点の脆弱性の影響を受けます。 CVE-2016-2183, CVE-2016-5546, CVE-2016-5547, CVE-2016-5548, CVE-2016-5549, CVE-2016-5552, CVE-2017-3231, CVE-2017-3241, CVE-2017-3252, CVE-2017-3253, CVE-2017-3259, CVE-2017-3260,

	CVE-2017-3261, CVE-2017-3272, CVE-2017-3289 Oracle Java をご利用のお客様は、クライアントおよび サーバサイドの Java 実行環境のバージョンに対する、最新 update を適用してください。 ただし、Java8 Update131 において、MD5 署名付き JAR ファイルの 署名検証では JAR を署名されていないものと見なす仕様変更があり、 下記の画面において正常に動作しない場合があります。 ・ detradeII 送受信アプレット ・ JOB 定義アプレット 上記に該当する場合、 myHULFT(https://his.hulft.com/mypage/login/login/)より 提供されるパッチの適用で回避可能です。 発生条件や回避方法などの詳細については、「3.対応パッチの提供」 および後述の「Java8Update131 においてアプレット起動エラーが発 生する問題」をご参照ください。 ＜HDC-EDI Manager＞ 影響ありません。
iDIVO	影響ありません。
SIGNAlert	影響ありません。

3.対応パッチの提供

myHULFT(https://his.hulft.com/mypage/login/login/)にログイン後に[製品情報]-[ツール/サンプル/ベータ版]に進んだ後、 カテゴリに[修正パッチ]を選択して検索してください。
ご利用の deTradeII 同梱 EDI Base バージョンとパッチのダウンロード名称は以下のとおりです。

deTradeII 同梱 **EDI Base Ver.**	**ダウンロード名称**
4.6.0	detradeII_SignPatch460 **サイズ**: 64,238 **バイト**
4.3.0～4.5.0	detradeII_SignPatch 430-450 **サイズ**: 63,228 **バイト**
3.9.1～4.2.0	detradeII_SignPatch 391-420 **サイズ**: 63,213 **バイト**

○パッチ適用手順
入手された zip に同梱のパッチリリースノート記載手順に従い、適用をお願いいたします。

【改訂履歴】

2017 年 4 月 28 日	初版作成

以上

2017 年 4 月 28 日

お客様各位

株式会社 セゾン情報システムズ
HULFT 事業部

Java 8 Update 131 においてアプレット起動エラーが発生する問題

HDC-EDI Base E2X/B2B/B2B LE（以降、EDI Base と記載）の Java アプレットを使用している画面を Oracle Java 8 Update 131 の環境で操作した場合に、セキュリティ例外のエラーによってアプレットの起動が失敗する事象を確認いたしました。

【本事象が起きる操作】

1） deTradeII のクライアント送受信機能
2） EDI Base 運用画面のメニュー[定義情報]－[JOB 定義]機能

つきましては、本事象の原因および対処方法を、下記のとおりご案内いたしますので、ご対応をお願いします。また、取引先様などへの影響の大きい1）のケースでは deTradeII 用にパッチを提供いたします。

ご不明な点などございましたら、貴社担当営業またはサポート契約を締結されているお客様はテクニカルサポートセンターまで、ご遠慮なくお問い合せください。
今後とも弊社ならびに弊社製品をよろしくお願い申し上げます。

記

1.現象

以下の操作にてセキュリティ例外のエラーが表示されアプレットの起動に失敗します。

1） deTradeII クライアント端末でのダウンロード／アップロードの操作を行うと以下の画面が表示されます。

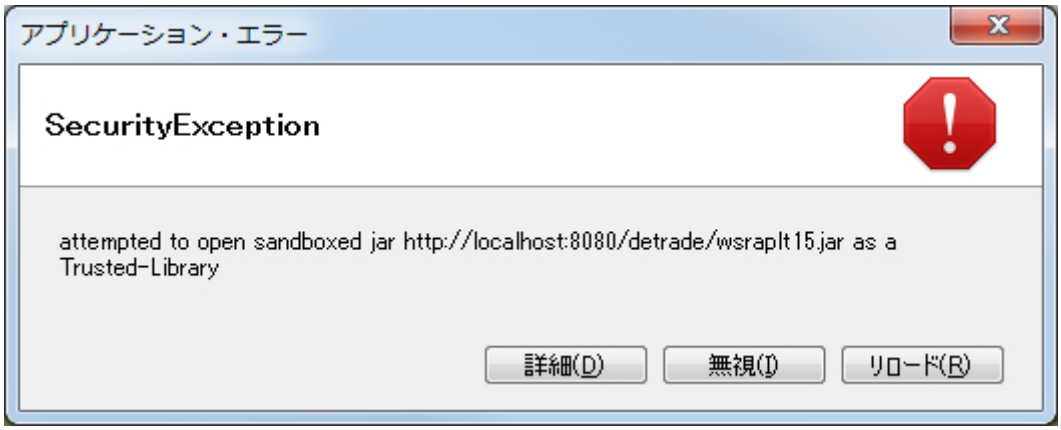

図 1：deTradeII 送受信アプレット起動エラー

2） EDI Base 運用画面にて JOB 定義アプレットを起動すると以下の画面が表示されます。

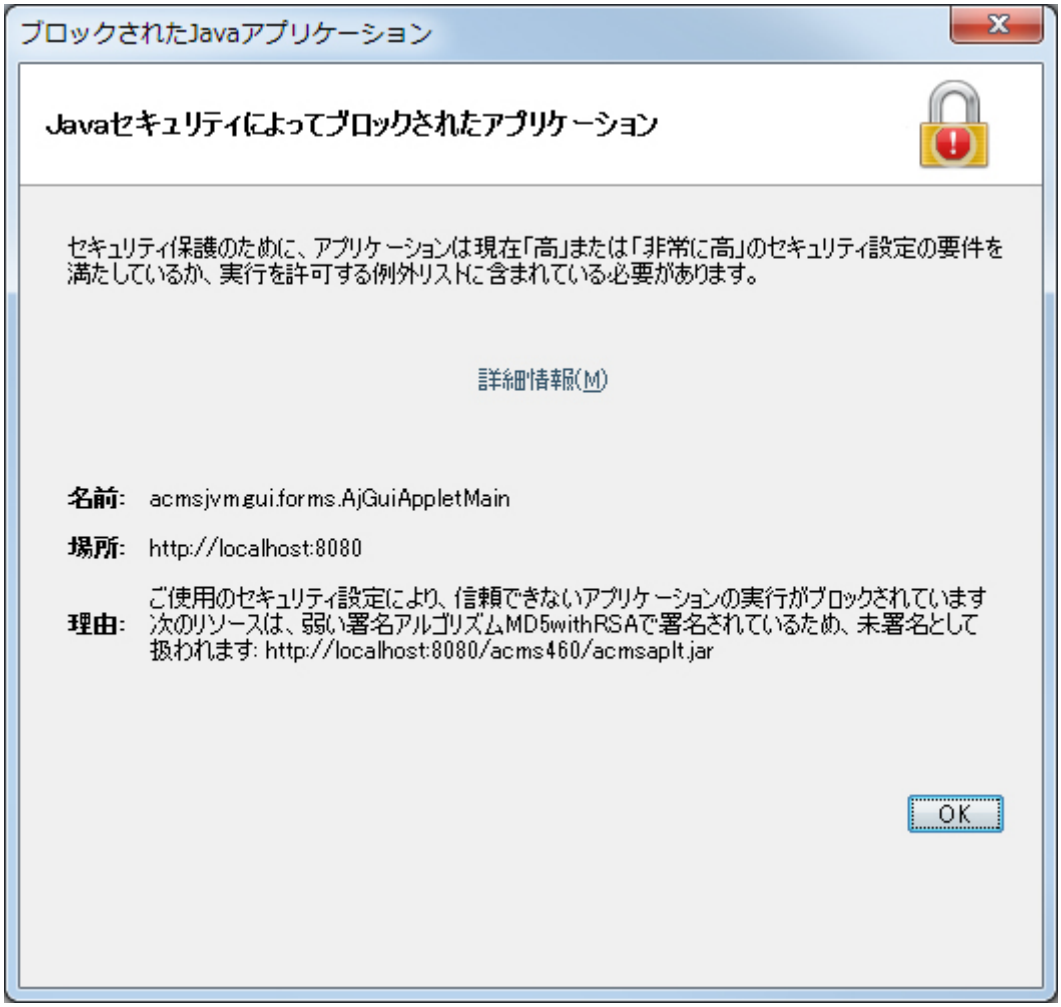

図 2：EDI Base JOB 定義アプレット起動エラー

2.原因

Oracle Java 8 Update 131 CPU（Critical Patch Update）が 2017 年 4 月 18 日にリリースされました。本 CPU では MD5 署名付き JAR ファイルの署名検証では JAR を署名されていないものと見なす仕様変更が行われました。

Oracle Java 8 Update 131 のリリースノート

This JDK release introduces a new restriction on how MD5 signed JAR files are verified. If the signed JAR file uses MD5, signature verification operations will ignore the signature and treat the JAR as if it were unsigned. 引用： http://www.oracle.com/technetwork/java/javase/8u131-relnotes-3565278.html MD5 added to jdk.jar.disabledAlgorithms Security property

EDI Base 製品が同梱する一部の弊社署名済みアプレットには MD5 で署名が行われているものが存在します。また、お客様が独自にアプレットへ署名された場合において署名時に使用した jarsigner コマンドのバージョンによっては MD5 で署名される場合がございます。

これらのアプレットモジュールを Oracle Java（JRE） 8 Update 131 で起動すると仕様変更によりアプレットがセキュリティ例外により起動エラーとなります。

MD5 署名済みのアプレット

以下のバージョンにて同梱するアプレットが対象となります。

deTradeII 送受信アプレット	EDI Base Ver.4.2.0 以前のご利用時、または、EDI Base Ver.4.3.0 以降の JRE6 用アプレットご利用時(※)
JOB 定義アプレット	EDI Base のすべてのバージョン

※ EDI Base Ver.4.3.0 以降では、取引先様クライアント端末にてアプレットが使用する JRE のデフォルトは「JRE 7 以上」となります。取引先様環境の要件が「JRE 6」を許容する必要がある場合に以下の設定を行うと「JRE6 用アプレット」が使用できるようになります。

JRE6 用アプレット使用の設定

WAS 側の detrade.properties が以下の設定になっている場合

dtc.client_jre_version=15

3.対処方法

本事象が発生する場合には、以下の方法で対処をお願いいたします。

1） deTradeII 送受信アプレット起動エラーへの対処方法

deTradeII のサーバ側のアプレットモジュールの差し替え

■弊社署名済みのデフォルトの送受信アプレットをご使用の場合
弊社が提供する差し替え版アプレットの適用をお願いします。

■お客様が独自に署名されたアプレットをご利用の場合
現在ご使用のアプレットは、JDK6 以前で同梱の jarsigner コマンドを使用して署名を行った可能性があります。以下の手順に従ってアプレットの差し替えをお願いします。

手順 1） deTradeII クライアント(detrade.war)を再デプロイ
手順 2） JDK7 以上に同梱の jarsigner コマンドを使用してアプレットに署名
手順 3） 新しく署名したアプレットを既存のアプレットと差し替え

署名の方法は、製品に同梱している「DetradeCustomizeGuide.pdf　第 7 章　送受信 Applet の署名」をご覧ください。

2）JOB 定義アプレットへの対処方法

EDI Base の運用画面として利用しているクライアント端末の JRE に、JRE 8 Update 121 以前のバージョンを適用する

EDI Base の運用画面として利用しているクライアント端末の JRE を、本 JRE 仕様変更が適用される以前のバージョンを適用していただくようお願いします。
万が一、JRE のバージョンが戻せない場合は、アプレットを使わないブラウザによる運用画面での操作、あるいは情報登録コマンドからの登録操作で代替していただけますようお願いします。
尚、現時点では、本件に関するパッチの提供予定はございません。EDI Base の次期バージョンにて対応を予定しています。

以上