NTTデータ・セキュリティ株式会社

Oracle Sun Java Deployment Toolkit の launch()メソッドにおける 引数検証処理の脆弱性(CVE-2010-0886)に関する検証レポート

2010/4/19

NTT データ・セキュリティ株式会社
辻 伸弘

【概要】

Oracle 社の Sun Java Deployment Toolkit(以下、SJDT)の launch()メソッドに引数検証処理の脆弱性（CVE-2010-0886）が存在することが発見されました。
この脆弱性により、細工された Web ページの閲覧などで、任意のコードが launch()メソッドを介して javaws ユーティリティに送信される危険性があります。
この脆弱性の利用例としては、「-J」パラメータの悪用により、任意の Jar ファイルが実行されることが挙げられます。
想定される被害としては、情報窃取、改ざん、または、悪意あるプログラムをシステム内にインストールされることが考えられます。

また、この脆弱性を利用した攻撃が各所から報告されています。

今回、この SJDT の脆弱性（CVE-2010-0886）の再現性について検証を行いました。

【影響を受けるとされているシステム】

・JDK および JRE 6 Update 19　およびそれ以前

【対策案】

Oracle 社から、修正されたバージョンのソフトウェアがリリースされています。
充分な検証の後、運用に支障をきたさないことをご確認の上、最新バージョンへのアップデートを行うことが推奨されます。

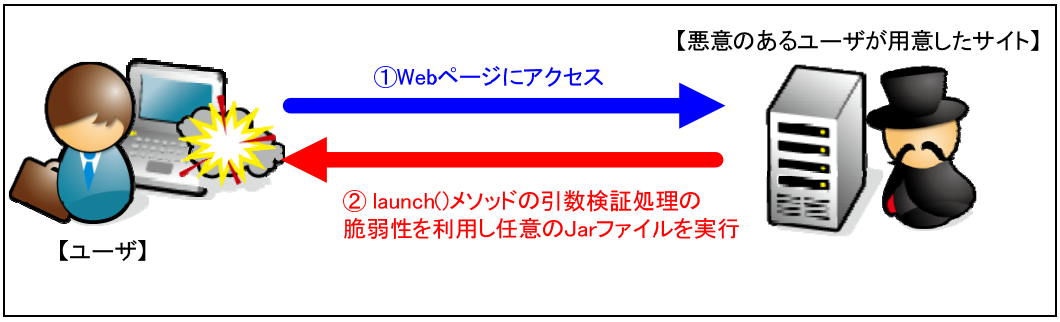
http://java.sun.com/javase/downloads/index.jsp

【参考サイト】

Oracle Security Alert CVE-2010-0886
http://www.oracle.com/technology/deploy/security/alerts/alert-cve-2010-0886.html

JVNVU#886582 - Oracle Sun Java　Deployment Toolkit に引数の検証処理に問題
https://jvn.jp/cert/JVNVU886582/index.html

【検証イメージ】



【検証ターゲットシステム】

WindowsXP 上にインストールされた Java 6 Standard Edition update 17

NTTデータ・セキュリティ株式会社

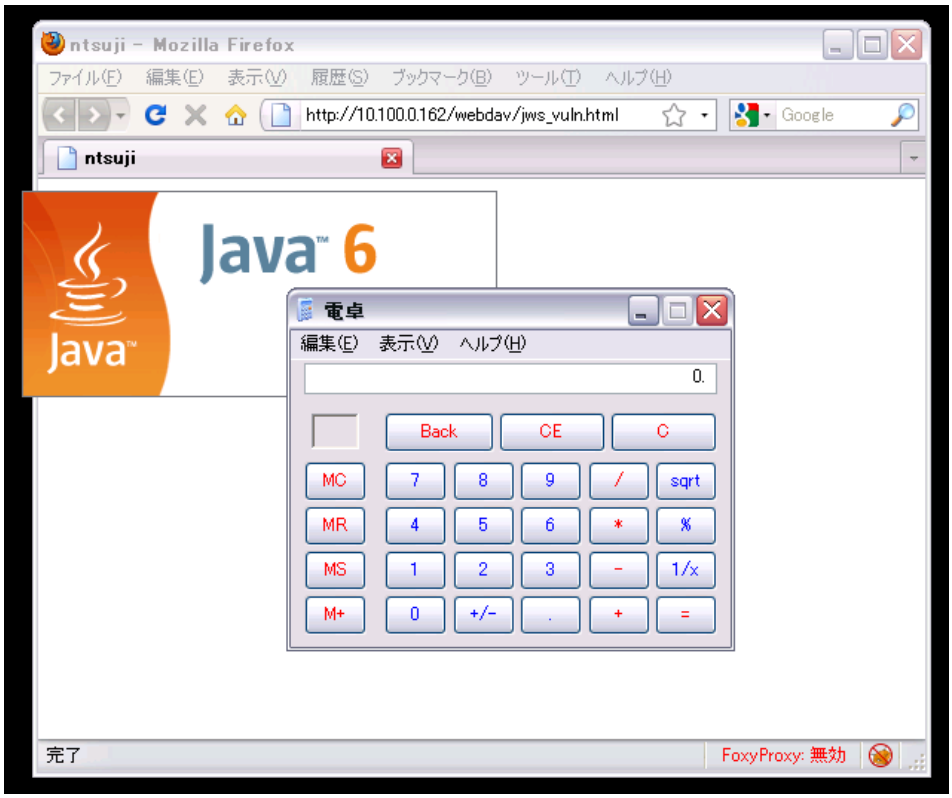
【検証概要】

ターゲットシステムに、細工した Web コンテンツをロードさせることで任意の Jar ファイルを実行させます。
今回の検証に用いた Jar ファイルは、ターゲットシステム上で「calc.exe」（電卓）を起動するものです。

【検証結果】

下図が示すように、細工した Web コンテンツにアクセス後、ターゲットシステム上で電卓が起動しました。これにより、脆弱性を利用し、ターゲットシステム上で任意の Jar ファイルが実行可能であると言えます。

ターゲットシステムの電卓の起動に成功した画面



＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】

NTT データ・セキュリティ株式会社
営業企画部
TEL：03-5425-1954
http://www.nttdata-sec.co.jp/