NTTデータ 先端技術株式会社

Oracle Java SE JDK7 および JRE7 のサンドボックス迂回により任意のコードが実行される脆弱性(CVE-2012-4681)に関する検証レポート

2012/8/30
2012/9/3 更新
NTT データ先端技術株式会社
辻 伸弘
小田切 秀暁
小松 徹也

【概要】

Oracle Java SE JDK7 および JRE7 に、リモートより任意のコードが実行される脆弱性が発見されました。 本脆弱性は、Java のサンドボックス機能を制御するセキュリティマネージャクラスを細工したコードにより無効化することにより、Java のセキュリティ機構を迂回されることにより発生します。

2012 年 8 月 29 日時点において Oracle 社から脆弱性への対策、回避策などのアナウンスはありません。また、本脆弱性を利用した Poison Ivy を使用した攻撃も観測されています。本脆弱性及び Poison Ivy を使用した攻撃が観測されていること、攻撃そのものが容易でありシステムに与える影響も大きいことから、本脆弱性(CVE-2012-4681)について再現性を検証いたしました。

【影響を受けるとされているシステム】

- Oracle Java JDK and JRE 7 Update 6 以前
(2012 年 8 月 29 日時点)

【対策案】

2012 年 8 月 29 日時点において、Oracle 社から本脆弱性を修正するバージョンはリリースされておりません。攻撃が成立する機会を減らすため、以下の対応が考えられます。

- ウイルス対策ソフトの定義ファイルを最新にする
- 不必要な Web サイトにアクセスしない
- クライアントに余計な通信を許可しない

上記対応は、普段から実施いただくことを推奨いたします。
また、業務等で Java が必要なサイト以外は、一時的に使用しているブラウザの Java プラグインを無効化することも対策となります。

なお、Oracle 社から本脆弱性を修正したバージョンがリリースされた際にはご利用環境への影響を確認の上、アップデートいただくことを推奨いたします。

Java SE ダウンロードサイト
http://www.oracle.com/technetwork/java/javase/downloads/index.html

2012 年 9 月 3 日追記：
Oracle 社から、修正プログラム（Oracle Java JDK and JRE 7 Update 7）がリリースされています。十分な検証の後、運用に支障をきたさないことをご確認の上、修正プログラムの適用を行なうことが推奨されます。
http://www.oracle.com/technetwork/java/javase/7u7-relnotes-1835816.html

修正プログラムを適用した以下のシステムに対して再度検証を行った結果、脆弱性の再現ができないことが確認されました。
・Windows XP SP3
・Java SE JRE 7 Update 7
上記の環境で、以下のブラウザを用いました。
・Internet Explorer 7
・Firefox 14
・Google Chrome 21

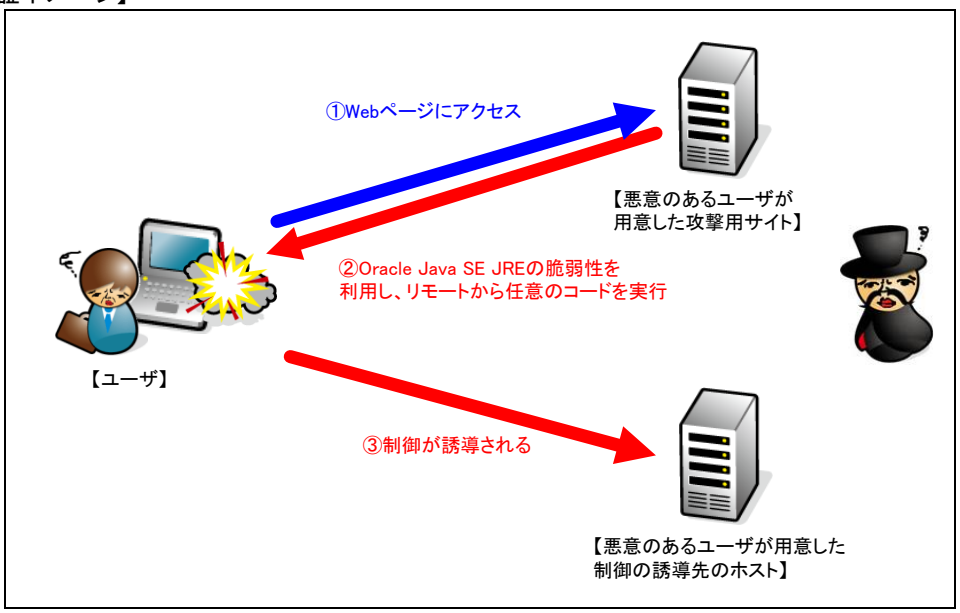
【参考サイト】
CVE-2012-4681
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2012-4681

JVNTA12-240A: Oracle Java 7 に脆弱性
http://jvn.jp/cert/JVNTA12-240A/

FireEye 社 blog(英語)
http://blog.fireeye.com/research/2012/08/zero-day-season-is-not-over-yet.html

2012 年 9 月 3 日追記：
Oracle Security Alert for CVE-2012-4681
http://www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715.html

【検証イメージ】



【検証ターゲットシステム】
・Windows XP SP3
・Java SE JRE 7 Update 6

上記環境で以下のブラウザを介して攻撃が成立することを確認しました。
・Internet Explorer 7
・Firefox 14
・Google Chrome 21

【検証概要】
ターゲットシステム上で、悪意のあるユーザが作成した Web ページを閲覧させることで、攻撃コードを実行させます。それによって、ターゲットシステムにおいて任意のコードを実行させます。
ターゲットシステムは、悪意のあるユーザが用意したホストに制御が誘導されます。

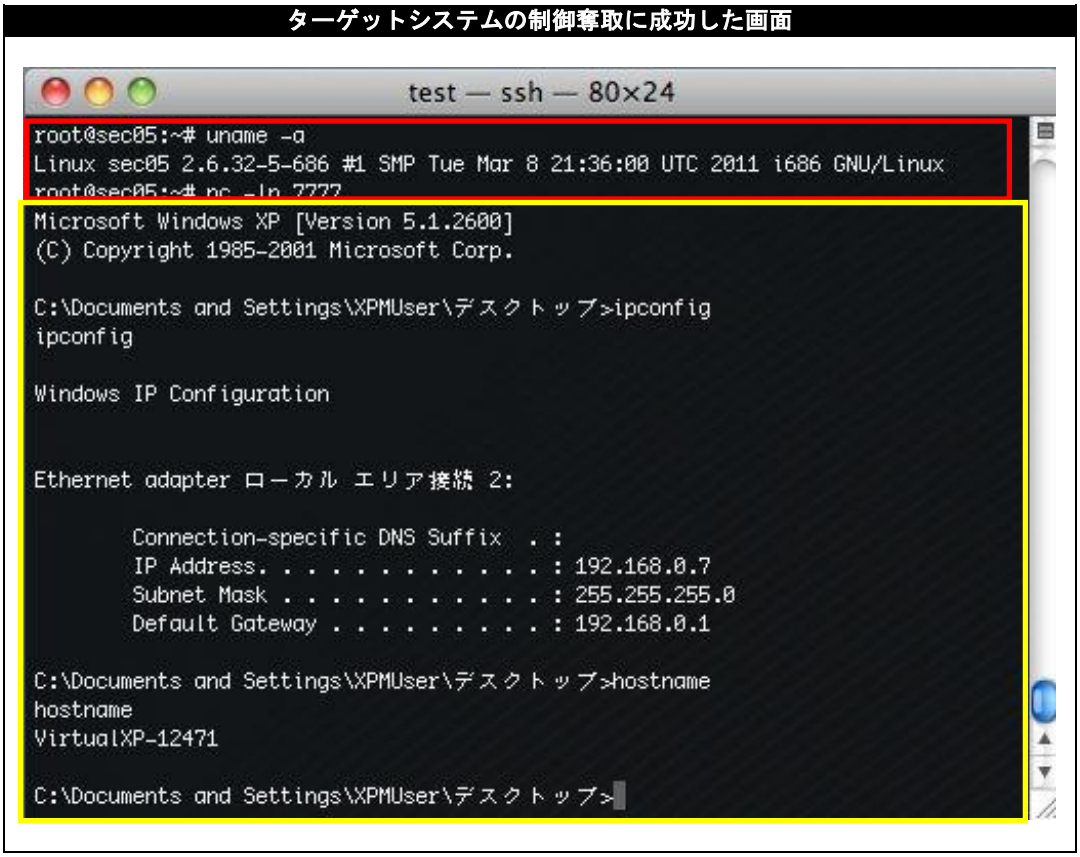
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムが操作可能となります。
** 誘導先のシステムは Debian です。*

【検証結果】

下図は、攻撃後の誘導先のシステム画面です。

下図の赤線で囲まれている部分の示すように、誘導先のコンピュータ（Debian）のターミナル上にターゲットシステム（Windows XP）のプロンプトが表示されています。
黄線で囲まれている部分の示すように、ターゲットシステムにおいて、コマンドを実行した結果が表示されています。これにより、ターゲットシステムの制御の奪取に成功したと言えます。

ターゲットシステムの制御奪取に成功した画面



＊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 データ先端技術株式会社
セキュリティ事業部　営業担当　サービス企画戦略グループ
TEL：03-5859-5422
http://security.intellilink.co.jp