NTTデータ・セキュリティ株式会社

Adobe Flash Player の authplay.dll の脆弱性(CVE-2011-0609)に関する検証レポート

2011/3/29
NTT データ・セキュリティ株式会社
辻 伸弘
小田切 秀暁

【概要】

Adobe 社の Flash Player に脆弱性（CVE-2011-0609）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、ローカルユーザと同じ権限が奪取される危険性があります。
想定される被害としては、ローカルユーザ権限での情報取得、改ざん、または、ワームやスパイウェアなどの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、当該脆弱性を利用し、不正な Flash ファイルを埋め込んだ Excel ファイル(.xls)を用いた標的型攻撃が発生しています。
不正なファイルの影響を緩和するために、マイクロソフトの「脆弱性緩和技術導入ツール（EMET)」ツールを使用して Excel に「データ実行防止（DEP:Data Execute Prevention)」及び「アドレス空間配置のランダム化（ASLR: Address space layout randomization)」を設定することが可能です。

今回、この FlashPlayer の脆弱性（CVE-2011-0609）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】

- Windows、Macintosh、Linux 及び Solaris OS で動作する Adobe Flash Player 10.2.152.33 以前
- Chrome ブラウザ用の Adobe Flash Player 10.2.154.13 以前
- Android 用の Adobe Flash Player 10.1.106.16 以前
- Windows 及び Macintosh OS で動作する、Adobe Reader 及び Acrobat X (10.0.1)以前、10.x 及び 9.x に同梱されている Authplay.dll コンポーネント

【対策案】

当該脆弱性が修正された最新版 Adobe Flash Player にアップデートいただく事を推奨いたします。

- Windows、Macintosh、Linux 及び Solaris OS で動作する Adobe Flash Player 10.2.153.1
- Chrome ブラウザを Chrome version 10.0.648.134 以降にアップデート
- Android 用の Adobe Flash Player 10.2.156.12

【参考サイト】

Security update available for Adobe Flash Player
http://www.adobe.com/support/security/bulletins/apsb11-05.html
CVE-2011-0609
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0609

【検証イメージ】

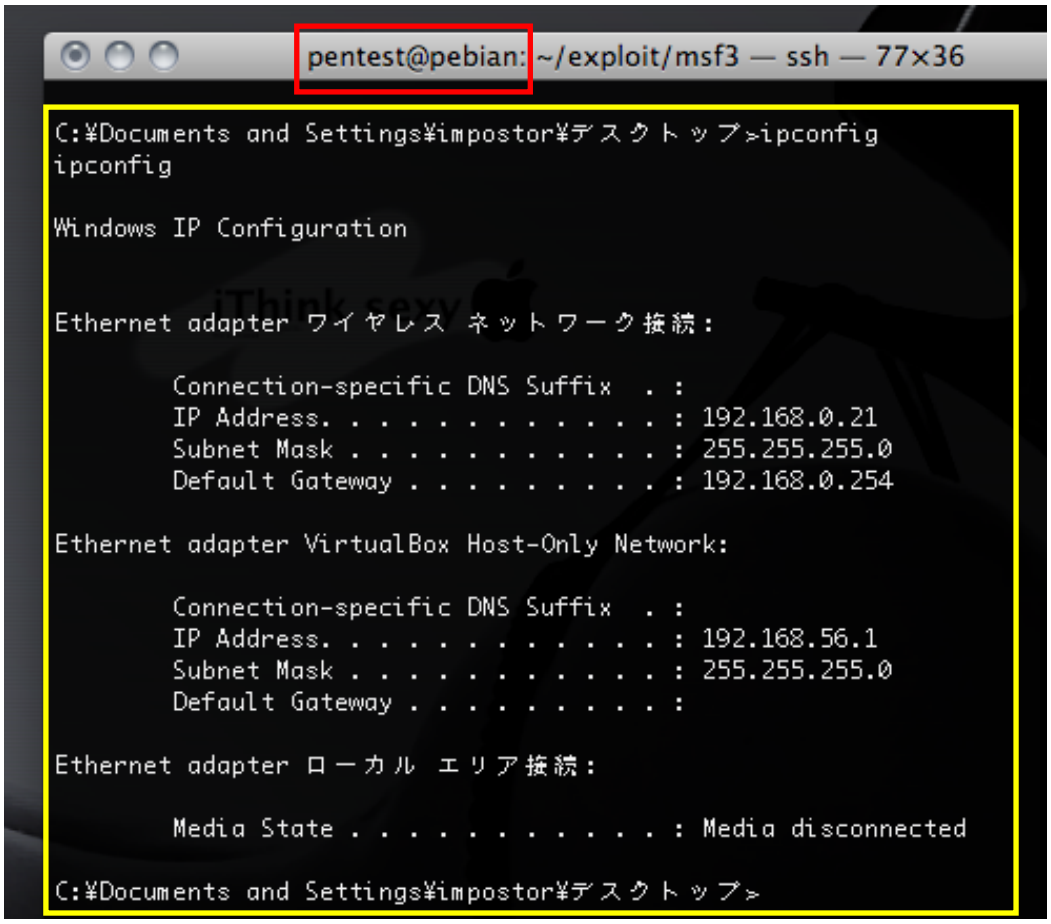
NTTデータ・セキュリティ株式会社

【検証ターゲットシステム】
Windows XP SP3 IE7 Flash Player 10.1.102.64

【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コードを実行させます。
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を操作可能となります。
＊ 誘導先のシステムは Debian 5.05 です。

【検証結果】
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）のコンソー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の奪取に成功した画面



NTTデータ・セキュリティ株式会社

＊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
企画部　広報グループ
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/