NTTデータ・セキュリティ株式会社

Adobe Reader, Acrobat および Flash Player の authplay.dll の脆弱性(CVE-2010-1297)に関する検証レポート

2010/6/11
NTT データ・セキュリティ株式会社
辻 伸弘

【概要】

Adobe Reader, Acrobat および Flash Player の authplay.dll に脆弱性が存在します。ActionScript Virtual Macnihe2(AVM2)に対して、細工された AVM2 newfunction 命令を実行させることにより任意のコードが実行される可能性があります。
この脆弱性を利用した攻撃は既に発生しており、Exploit コードもリリースされています。
この脆弱性により、細工された Web ページやドキュメント（Flash コンテンツは様々な文書形式に埋め込まれている可能性があります。）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。

今回、脆弱性（CVE-2010-1297）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】

・Adobe Flash Player 10.0.45.2 およびそれ以前
・Adobe Flash Player 9.0.262 およびそれ以前
・Adobe Reader and Acrobat 9.3.2 およびそれ以前
（注)Flash をサポートしている Photoshop、Photoshop Lightroom、Freehand MX および Fireworks なども影響を受ける可能性があります。

【対策案】

Adobe 社から、セキュリティアップデートが公開されています。
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。
また、Adobe Reader および Acrobat の更新は、2010 年 6 月 29 日までに公開される予定です。
こちらの影響の軽減策としては、authplay.dll の削除、変名、もしくは、移動が Adobe 社より提示されています。（これらの対策を行った場合でも強制終了やエラーメッセージなどの表示がされます。）
authplay.dll の一般的なファイルパスは下記の通りです。

・Adobe Reader
C:¥Program Files¥Adobe¥Reader 9.0¥Reader¥authplay.dll

・Acrobat
C:¥Program Files¥Adobe¥Acrobat 9.0¥Acrobat¥authplay.dll

【参考サイト】

Adobe Flash Player 用のセキュリティアップデート公開
http://kb2.adobe.com/jp/cps/850/cpsid_85036.html

JVNDB-2010-001127 Adobe Reader および Acrobat における任意のコードを実行される脆弱性
http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-001127.html

JVNVU#486225 Adobe Flash ActionScript AVM2 newfunction 命令に脆弱性
http://jvn.jp/cert/JVNVU486225/index.html

CVE-2010-1297
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1297

NTTデータ・セキュリティ株式会社

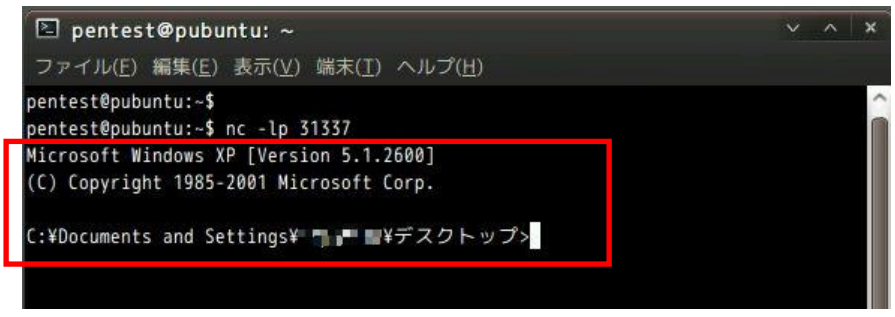
【検証イメージ】

【検証ターゲットシステム】
Windows XP SP3
Adobe Flash Player 10.0.45.2
Adobe Reader 9.3.2

【検証概要】
ターゲットシステムに、Web ブラウザを通じて細工した PDF ファイル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 Ubuntu 9.10 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（Ubuntu 9.10）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。
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



＊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/