NTTデータ・セキュリティ株式会社

Adobe Reader、及び、Acrobat の脆弱性（CVE-2009-2994）に関する検証レポート

2009/11/9
診断ビジネス部
辻　伸弘
松田　和之

【概要】

Adobe Reader、及び、Acrobat にバッファオーバーフローの脆弱性が存在することが発見されました。
この脆弱性により、Web ページの閲覧、HTML 形式の電子メールの表示、または、電子メールの添付ファイルなどの経路から細工された PDF ファイルを閲覧した場合に、そのローカルユーザと同じ権限が奪取される恐れがあります。
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、Adobe Reader、及び、Acrobat の脆弱性（CVE-2009-2994）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 Reader、Acrobat のバージョン 9.2 より前のバージョン
Adobe Reader、Acrobat のバージョン 8.1.7 より前のバージョン
Adobe Reader、Acrobat のバージョン 7.1.4 より前のバージョン

【対策案】

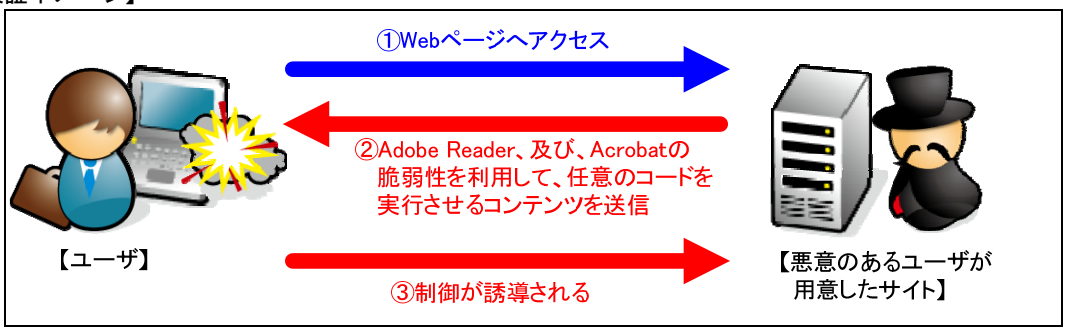
Adobe 社から、修正されたバージョンの Adobe Reader、及び、Acrobat がリリースされています。
充分な検証の後、運用に支障をきたさないことをご確認の上、最新バージョンへのアップデートを行うことが推奨されます。

http://www.adobe.com/jp/support/security/bulletins/apsb09-15.html

【参考サイト】

Adobe Reader および Acrobat 用セキュリティアップデート公開
http://www.adobe.com/jp/support/security/bulletins/apsb09-15.html
CVE-2009-2994
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2994

【検証イメージ】



【検証ターゲットシステム】

Adobe Reader 9.0 がインストールされた Windows XP

NTTデータ・セキュリティ株式会社

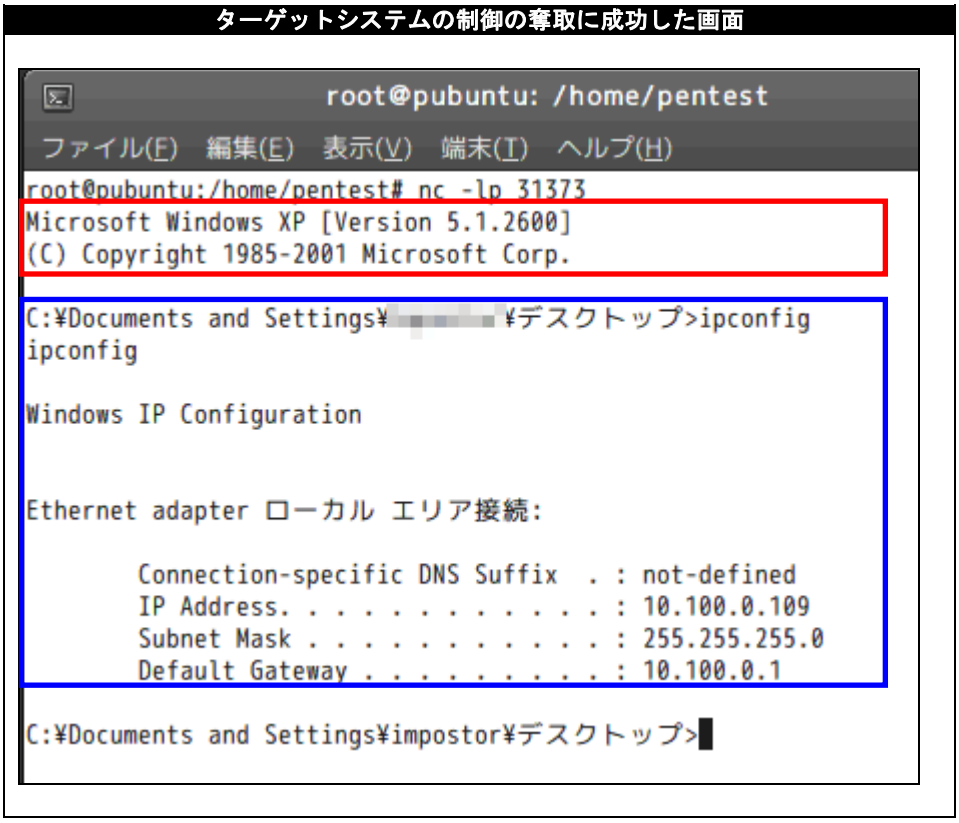
【検証概要】

ターゲットシステムに、細工した PDF ファイルを含む Web コンテンツを閲覧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 9.04 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）のコマンドプロンプト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。
青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



＊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/