NTTデータ先端技術株式会社

Adobe Reader および Acrobat における U3D の処理の脆弱性(CVE-2011-2462)に関する検証レポート

2012/1/17
NTT データ先端技術株式会社
辻 伸弘
渡邊 尚道

【概要】

Adobe Reader および Acrobat に、PDF ファイル内に組み込まれた U3D (Universal 3D) ファイルの処理に脆弱性が発見されました。U3D は 3D グラフィックを表現するために使用されるファイル形式です。本脆弱性はこの U3D の解析処理の際、ポインタを正しく初期化しないことにより発生します。

この脆弱性により、攻撃者が、細工した pdf ファイルを電子メールに添付し送信、または、何らかの方法でユーザを攻撃者の Web サイトに誘導し、細工した pdf ファイルを閲覧させることで、ローカルユーザと同じ権限を奪取できる危険性があります。

今回、この Adobe Reader および Acrobat の脆弱性 (CVE-2011-2462) 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アプリケーション】

-Windows、Macintosh 版 Adobe Reader X (10.1.1) 以前のバージョン
-Windows、Macintosh、Unix 版 Adobe Reader 9.4.6 以前のバージョン
-Windows、Macintosh 版 Adobe Acrobat X (10.1.1) 以前のバージョン
-Windows、Macintosh 版 Adobe Acrobat 9.4.6 以前のバージョン
*Android 版 Adobe Reader については、この脆弱性の影響を受けません。

【対策案】

当該脆弱性が修正された最新版 Adobe Reader および Acrobat にアップデートしていただく事を推奨いたします。本脆弱性は、それぞれ、10.1.2 または、9.4.7 以降にて対策済みです。

・アップデート方法
- Adobe Reader の場合
「ヘルプ」メニューの「アップデートの有無をチェック」から更新
または、以下のサイトから最新版をダウンロードしてください。
http://get.adobe.com/jp/reader/

- Adobe Acrobat の場合
以下のサイトから最新版をダウンロードしてください。
http://www.adobe.com/jp/downloads/updates/

アップデート以外の対処方法として、「Adobe Reader X」「Adobe Acrobat X」v10 以降においては、”保護モード”機能にて、本脆弱性の回避が可能です。
*保護モードはデフォルトで有効になっております。

【参考サイト】

APSA11-04: Adobe Reader および Acrobat に関するセキュリティ情報
http://kb2.adobe.com/jp/cps/926/cpsid_92600.html

APSB11-30 : Windows 版 Adobe Reader 9.x および Acrobat 9.x に関するセキュリティアップデート公開
http://kb2.adobe.com/jp/cps/927/cpsid_92703.html

NTTデータ先端技術株式会社

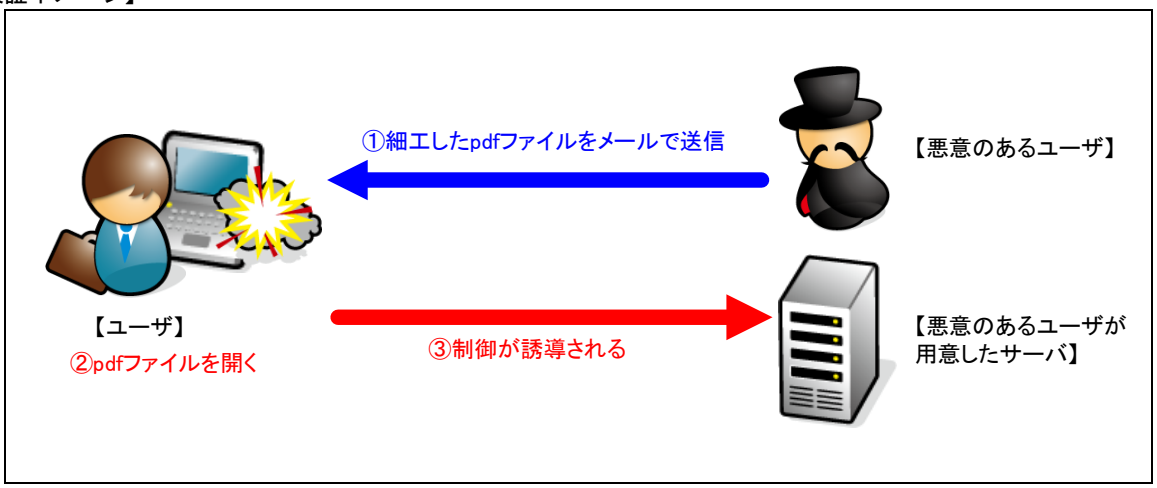
APSB12-01: Adobe Reader および Acrobat に関するセキュリティアップデート公開
http://kb2.adobe.com/jp/cps/928/cpsid_92823.html

CVE -CVE-2011-2462 (under review)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2462

National Vulnerability Database (NVD) National Vulnerability Database (CVE-2011-2462)
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-2462

Adobe Reader および Acrobat の脆弱性 (APSA11-04) について
http://www.ipa.go.jp/security/ciadr/vul/20111208-adobe.html

【検証イメージ】



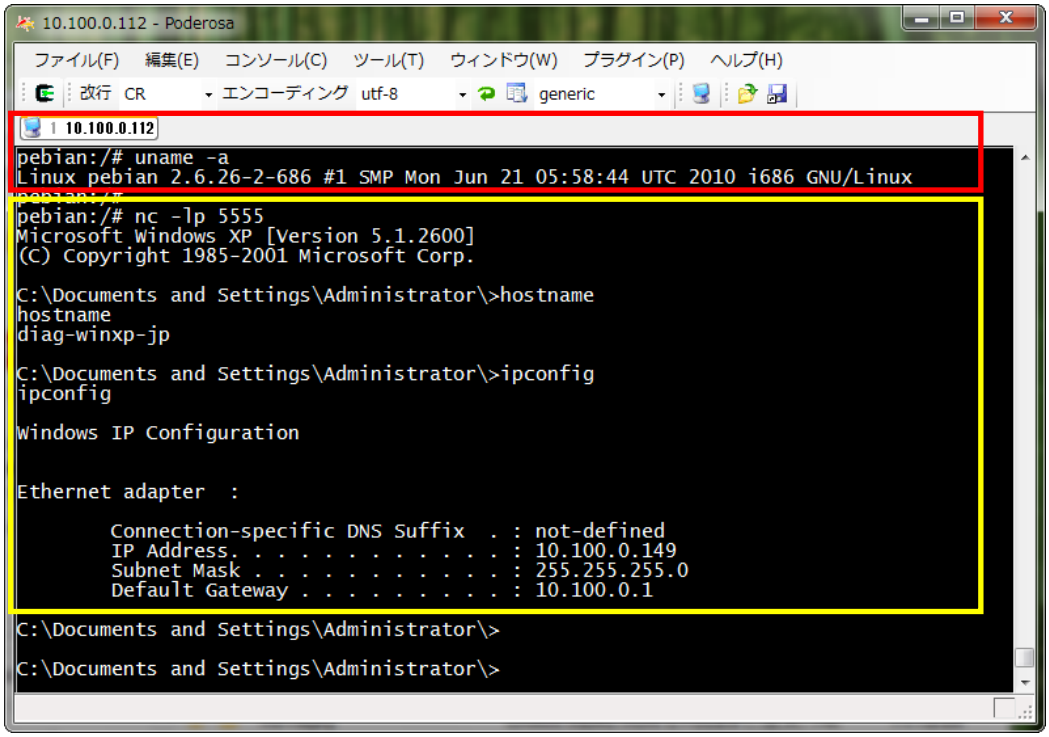
【検証ターゲットシステム】
Windows XP SP3 Adobe Reader 9.4.6

【検証概要】
ターゲットシステムにおいて、細工した pdf ファイルを開か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が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。

NTTデータ先端技術株式会社

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 データ先端技術株式会社
セキュリティ事業部　営業担当　営業企画グループ
TEL：03-5425-1954
http://security.intellilink.co.jp/