NTTデータ・セキュリティ株式会社

Adobe Reader と Acrobat における CoolType.dll のフォント解析コードに起因するバッファオーバーフローの脆弱性(CVE-2010-2883)に関する検証レポート

2010/10/1
NTT データ・セキュリティ株式会社
辻 伸弘
小田切 秀暁

【概要】

アドビシステムズ社の Adobe Reader 及び Acrobat に、リモートから攻撃可能なバッファオーバーフローの脆弱性が見つかっています。
この脆弱性により、任意のコードがリモートから実行される可能性があります。脆弱性は CoolType.dll に存在し、不正な Smart INdependent Glyplets (SING)テーブルを含む TTF フォントを解析すると発生します。

今回、脆弱性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】

Adobe Reader および Acrobat 9.3.4 およびそれ以前

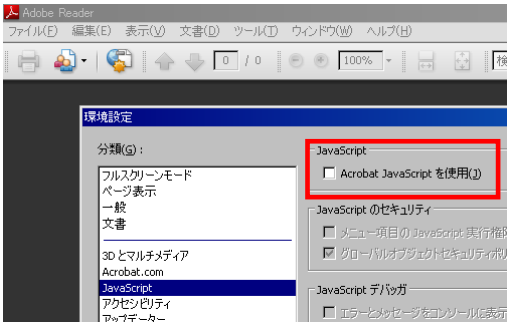
【対策案】

このレポート作成現在（2010 年 10 月 1 日）修正プログラムはリリースされていません。
なお、アドビシステムズ社から Adobe Reader と Acrobat の臨時セキュリティアップデートを 10 月 5 日（米国時間）公開し本脆弱性を含む複数の深刻な脆弱性に対処すると発表されています。
今回のアップデートは 10 月 12 日にリリースする予定の四半期アップデートの日程を前倒ししたリリースとなります。

また、以下の暫定回避策があります。

・ Adobe Acrobat および Adobe Reader の JavaScript を無効にする暫定回避策

Adobe Acrobat および Adobe Reader のメニューから
「編集」→「環境設定」→「JavaScript」→「Acrobat JavaScript を使用(J)」のチェックをはずす



・ EMET による暫定回避策

Adobe Systems から、Microsoft 社が提供しているツールである EMET (Enhanced Mitigation Experience Toolkit) v2.0 が有効であることが発表されています。EMET の詳細は以下の情報を参照ください。
http://blogs.technet.com/b/srd/
※WindowsXP は ASLR(Address Space Load Randomization)が使用できないため、この暫

定回避策をとることはできません。

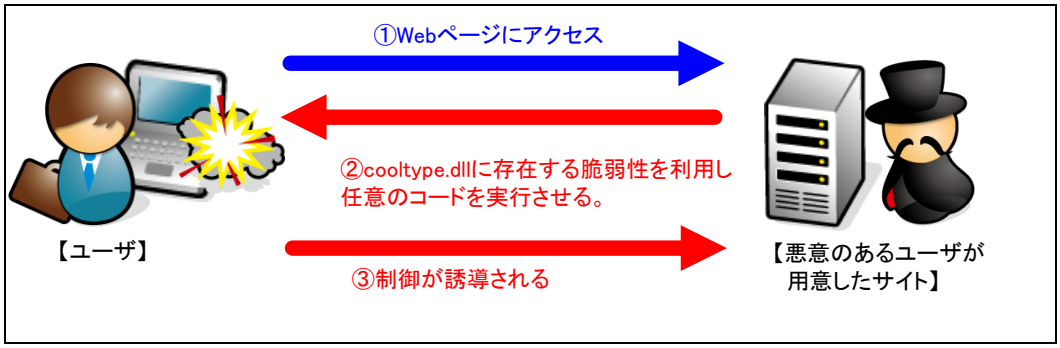
【参考サイト】

APSA10-02：Adobe Reader と Acrobat に関するセキュリティ情報
http://kb2.adobe.com/jp/cps/866/cpsid_86615.html

JVNTR-2010-24 Adobe Reader および Acrobat に脆弱性 (CVE-2010-2883, VU#491991)
http://jvn.jp/tr/JVNTR-2010-24/index.html

CVE-2010-2883
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2883

【検証イメージ】



【検証ターゲットシステム】

Windows XP SP3 上の Adobe Reader 9.3.4

【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 Debian GNU/Linux 5.05 です。

【検証結果】

下図が示すように、誘導先のコンピュータ（Debian GNU/Linux 5.05）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

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/