NTTデータ 先端技術株式会社

Adobe Flash Player のフォント解析における任意のコードが実行される脆弱性 (CVE-2012-1535)に関する検証レポート

2012/8/22
NTT データ先端技術株式会社
辻 伸弘
泉田 幸宏

【概要】

Adobe Flash Player に、リモートより任意のコードが実行される脆弱性が発見されました。この脆弱性は、Flash Player に細工されたフォントを解析させることで、システムへログオンしているユーザと同じ権限で任意のコードを実行させることが可能です。
この脆弱性を利用する Word 文書を装った不正なファイルが添付されたメールによる攻撃が観測されております。

Adobe 社では、Windows 版における脆弱性の優先度を最も高く設定しております。しかしながら Macintosh 版および Linux 版の Flash Player においても、脆弱性の影響を受けるバージョンを利用している場合、アップデートを実施することが推奨されております。

【影響を受けるとされているシステム】

- Windows、Macintosh 版の Adobe Flash Player 11.3.300.270 以前
- Linux 版の Adobe Flash Player 11.2.202.236 以前

【対策案】

Adobe 社より、この脆弱性を修正するバージョンがリリースされています。
当該脆弱性が修正されたバージョンにアップデートしていただくことを推奨いたします。

- Windows、Macintosh 版 Adobe Flash Player 11.3.300.271
- Linux 版 Adobe Flash Player 11.2.202.238

【参考サイト】

CVE-2012-1535
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1535

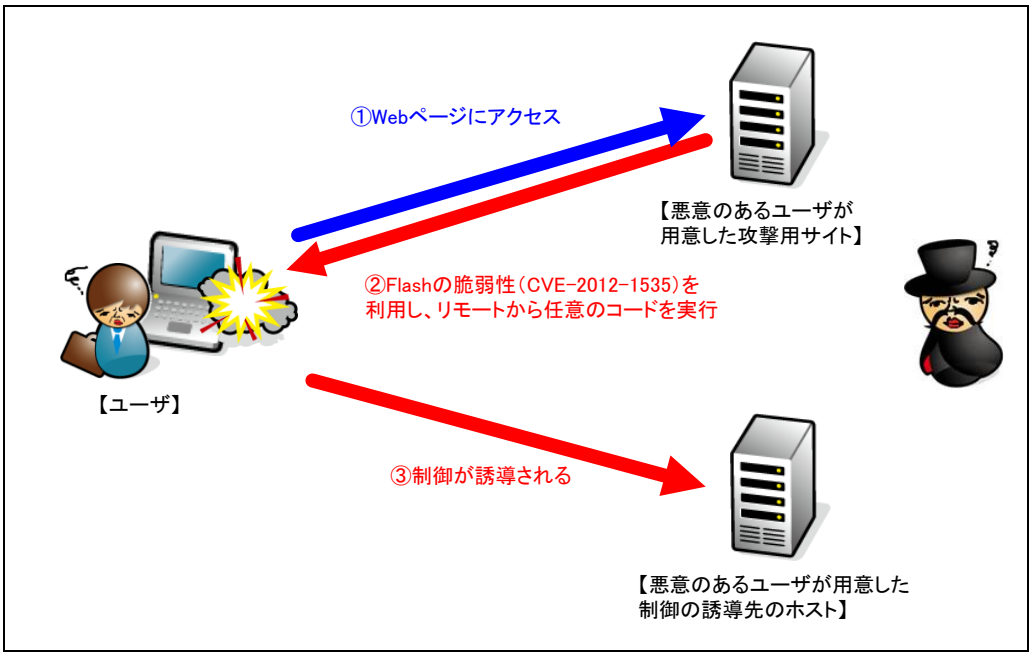
APSB12-18: Adobe Flash Player に関するセキュリティアップデート公開
http://helpx.adobe.com/jp/flash-player/kb/cq08150306.html

Adobe Flash Player の脆弱性の修正について(APSB12-18)(CVE-2012-1535)
http://www.ipa.go.jp/security/ciadr/vul/20120815-adobe.html

脆弱性「CVE-2012-1535」、バックドア型不正プログラムをもたらす
http://blog.trendmicro.co.jp/archives/5785

iPhone 5 Rumors Used as Bait for Adobe Exploit CVE-2012-1535 (英語)
http://www.symantec.com/connect/blogs/iphone-5-rumours-used-bait-adobe-exploit-cve-2012-1535

【検証イメージ】



【検証ターゲットシステム】
Windows XP SP3 Internet Explorer 6 Flash Player 11.3.300.270

【検証概要】
ターゲットシステム上で、悪意のあるユーザが作成した Web ページを閲覧させることで、攻撃コードを実行させます。それによって、ターゲットシステムにおいて任意のコードを実行させます。
ターゲットシステムは、悪意のあるユーザが用意したホストに制御が誘導されます。

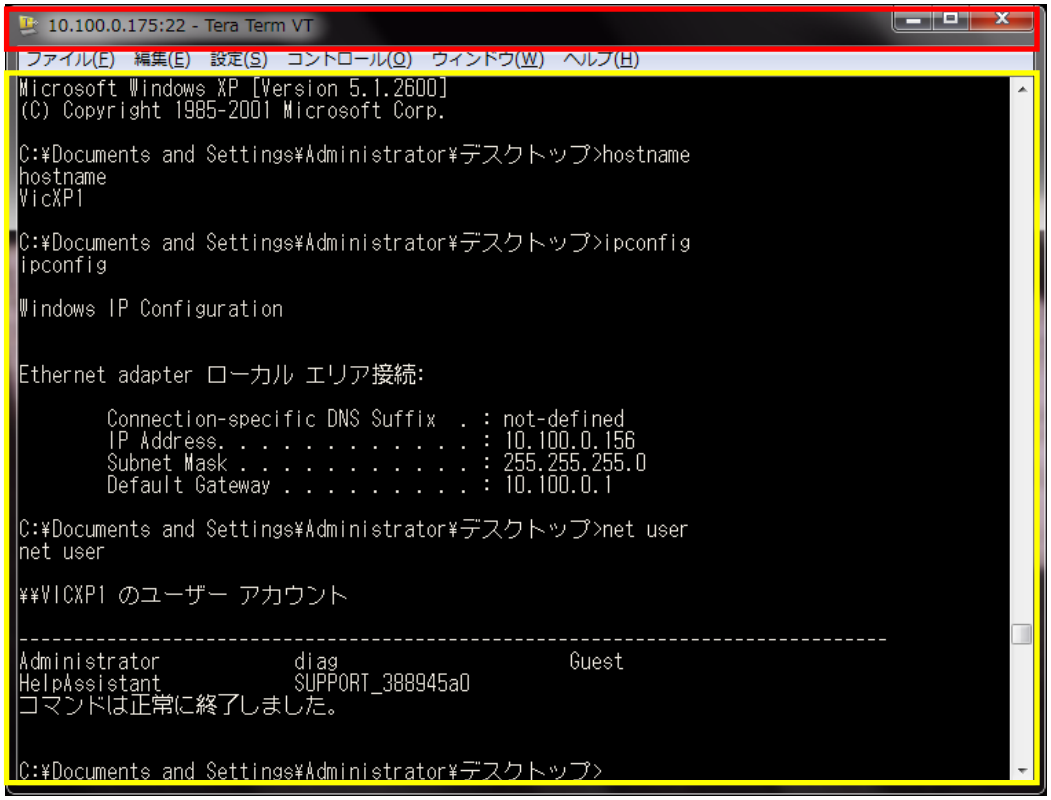
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムが操作可能となります。
＊ 誘導先のシステムは Debian です。

【検証結果】

下図は、攻撃後の誘導先のシステム画面です。

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）のターミナ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　サービス企画戦略グループ
TEL：03-5859-5422
http://security.intellilink.co.jp