NTT DATA
NTTデータ 先端技術株式会社

Adobe Flash Player のオブジェクト混乱の脆弱性(CVE-2012-0779)に関する検証レポート

2012/6/29
NTT データ先端技術株式会社
辻 伸弘
小田切 秀暁

【概要】

Adobe Flash Player にオブジェクト混乱の脆弱性（CVE-2012-0779）が存在します。この脆弱性は、RTMP _error メッセージの処理をする際にオブジェクトの混乱が引き起こされることに起因しています。

この脆弱性は 2012 年 5 月 4 日に Adobe 社からセキュリティ情報が公開されたものです。実際に細工された Microsoft Office ファイルを電子メールに添付した攻撃が観測されています。細工されたファイルには悪意のあるサイトの Flash コンテンツへのリンクが埋め込まれており、添付ファイルを開いたユーザと同じ権限を奪取されます。

今回、この Adobe Flash Player の脆弱性（CVE-2012-0779）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・アプリケーション】

- Flash Player 11.2.202.233 以前のバージョン
- Flash Player 11.1.115.7 以前のバージョン（Android 4.x）
- Flash Player 11.1.111.8 以前のバージョン（Andoroid 3.x/2.x）

【対策案】

Adobe 社より、この脆弱性を修正した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いただくことを推奨いたします。

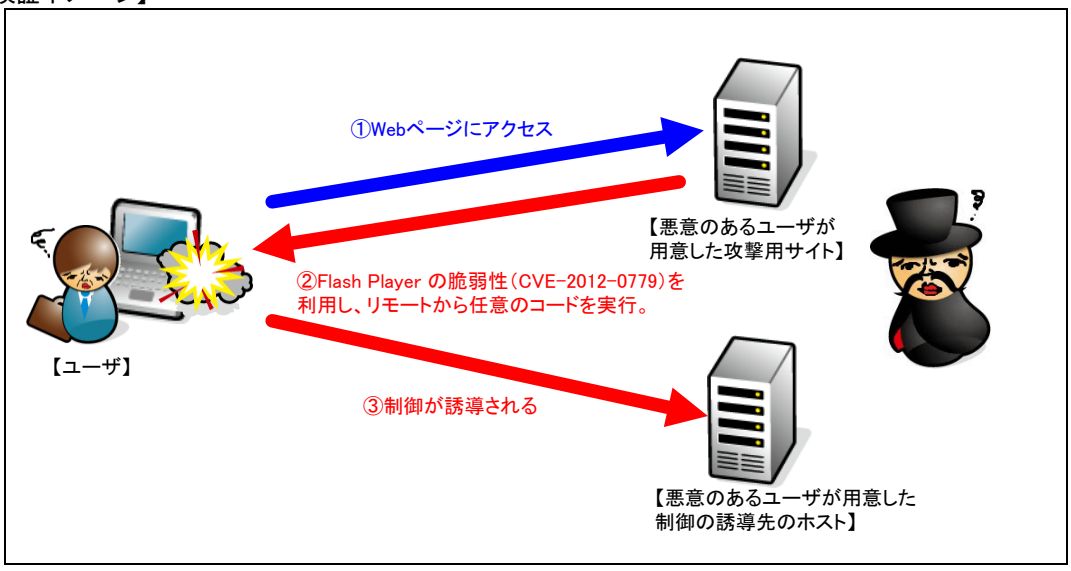
- Flash Player 11.2.202.235 以降
- Flash Player 11.1.115.8 以降（Android 4.x）
- Flash Player 11.1.111.9 以降（Andoroid 3.x/2.x）

【参考サイト】

CVE-2012-0779
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0779

Adobe - Security Bulletins: APSB12-09
http://www.adobe.com/support/security/bulletins/apsb12-09.html

【検証イメージ】



NTT DATA
NTTデータ 先端技術株式会社

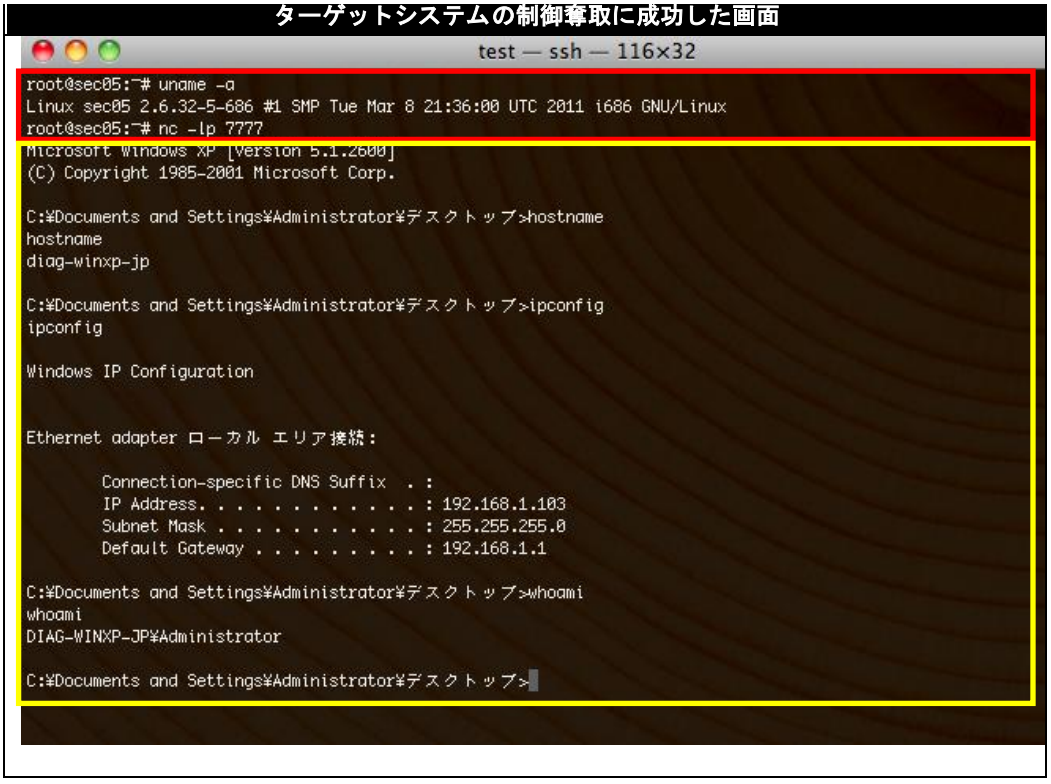
【検証ターゲットシステム】
Windows XP SP3 Internet Explorer 7 Flash Player 11.1.102.63

【検証概要】
ターゲットシステムに、悪意のあるユーザが用意した 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 6.0 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。

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/