NTTデータ先端技術株式会社

Adobe Flash Player のメモリ破損の脆弱性 (CVE-2012-0754)に関する検証レポート

2012/3/12
NTT データ先端技術株式会社
辻 伸弘
川島 祐樹
小田切 秀暁

【概要】

Adobe Flash Player にリモートからの攻撃を可能にするメモリ破損の脆弱性が発見されました。これにより、攻撃者は、 細工した Flash ファイルを処理させることで、攻撃可能な状態となります。この脆弱性を利用して攻撃者はターゲットホスト上で任意のコードの実行が可能です。
本レポート執筆時点で、これ以上詳細な情報は公開されていません。

この脆弱性を悪用して、攻撃者はターゲットホスト上で任意のコードの実行が可能です。想定される被害としては、奪取されたユーザ権限による情報取得、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 Flash Player の不特定のメモリ破損の脆弱性 (CVE-2012-0754)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】

- Flash Player 11.1.102.55 以前のバージョン
- Flash Player 11.1.112.61 以前のバージョン (Android)
- Flash Player 11.1.111.5 以前のバージョン (Android)
- Flash Player 11.1.102.55 以前のバージョン (Chrome)

【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おります。
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。

- Flash Player 11.1.102.62 以降
- Flash Player 11.1.115.6 以降 (Android)
- Flash Player 11.1.111.6 以降 (Android)
- Flash Player 11.1.102.62 以降 (Chrome)

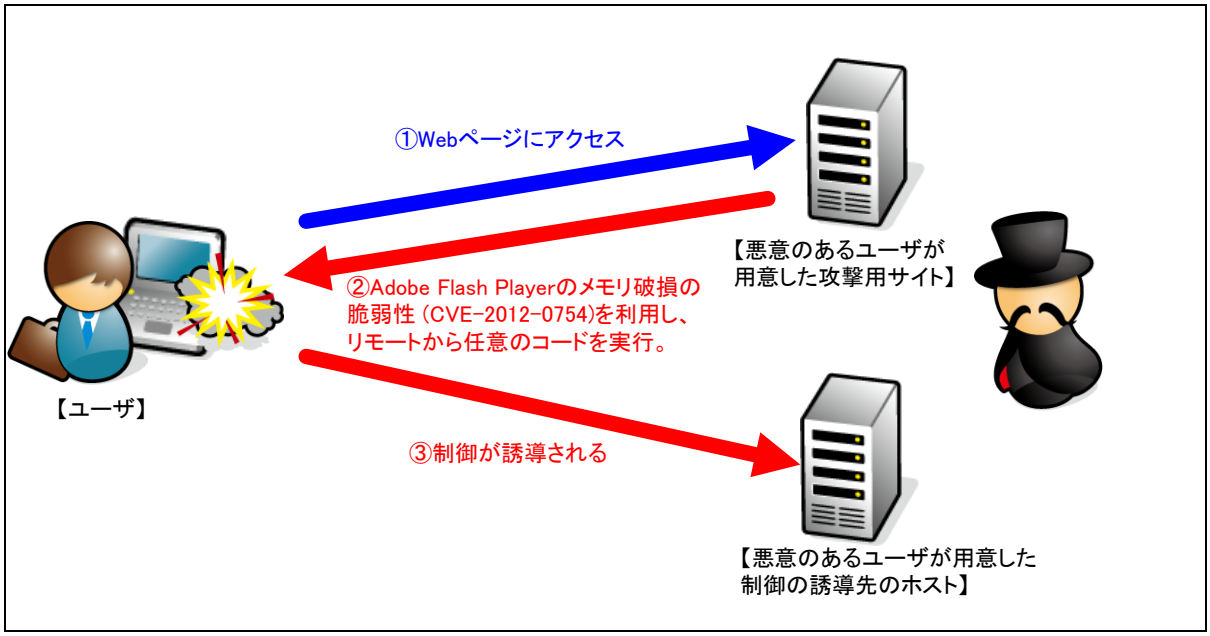
【参考サイト】

Security update available for Adobe Flash Player
http://www.adobe.com/support/security/bulletins/apsb12-03.html

CVE-2012-0754
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0754

NTTデータ先端技術株式会社

【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 11.1.102.55
Windows XP SP3 Internet Explorer 7 Flash Player 11.1.102.55
Windows XP SP3 Internet Explorer 8 Flash Player 11.1.102.55
Windows XP SP3 Internet Explorer 6 Flash Player 10.3.183.10
Windows XP SP3 Internet Explorer 7 Flash Player 10.3.183.10
Windows XP SP3 Internet Explorer 8 Flash Player 10.3.183.10

【検証概要】

ターゲットシステムに、Web ページを閲覧させ、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。

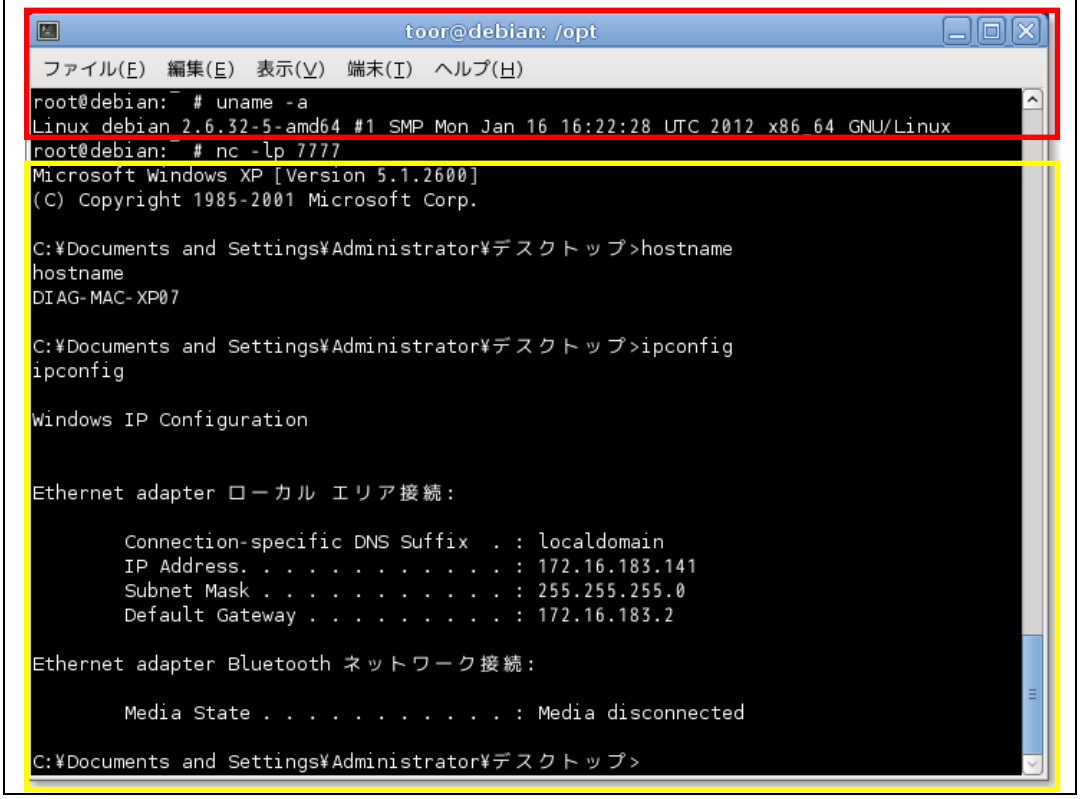
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムが操作可能となります。
＊ 誘導先のシステムは Debian 6.04 です。

NTTデータ先端技術株式会社

【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　営業企画グループ
TEL:03-5425-1954
http://security.intellilink.co.jp/