SoftBank Technology

ソフトバンク・テクノロジー株式会社

脆弱性調査レポート

Flash Player の脆弱性により、リモートから任意のコードが実行可能な脆弱性（CVE-2015-0359）（APSB15-06）に関する調査レポート

【概要】

アドビ システムズ社の Flash Player に、リモートより任意のコードが実行される脆弱性（CVE-2015-0359）の攻撃コードが発見されました。

この脆弱性は、Byte Array クラスに解放済みメモリ使用（Use-After-Free）の欠陥が存在しており、これにより Flash Player は任意のコードが書き込まれたメモリアドレスを呼び出すことが可能です。

この脆弱性を利用した攻撃が成立した場合、リモートから Flash Player を実行するアプリケーションの実行権限を奪取される危険性があります。

本レポート作成（2015 年 5 月 14 日）時点において、ベンダーより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（2015 年 4 月 14 日）。しかしながら、攻撃を成立させるためのコードが容易に入手可能であり、かつ脆弱性に対する攻撃が容易であること、また攻撃を受けた際にシステムへの影響が大きいことから、今回、この脆弱性（CVE-2015-0359）の再現性について検証を行いました。

【影響を受ける可能性があるシステム】

- Adobe Flash Player 17.0.0.134 とそれ以前のバージョン
- Adobe Flash Player 13.0.0.277 とそれ以前の 13.x バージョン
- Adobe Flash Player 11.2.202.451 とそれ以前の 11.x バージョン

【対策案】

アドビ システムズ社より、この脆弱性を修正するプログラムがリリースされています。

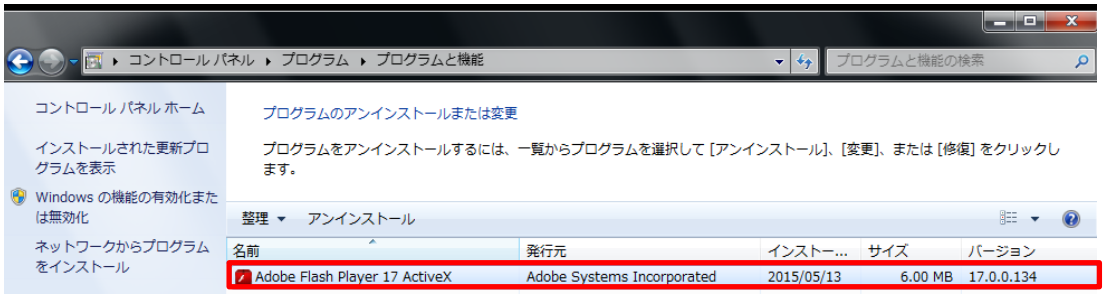
当該脆弱性の修正を含む最新のバージョンを適用していただくことを推奨いたします。

*本調査レポートの脆弱性の他に、4 月の更新にて修正された、CVE-2015-3043 を利用した攻撃が観測されており、最新の Flash Player バージョンに更新していただくことを推奨します。(2015/5/13 時点)

（参考：Adobe Flash Player の脆弱性対策について(APSB15-06)(CVE-2015-3043 等)）

【バージョン確認方法】

[コントロールパネル] – [プログラム] – [プログラムと機能] より Adobe Flash Player のバージョンを確認できます。



以下のサイトにて、現在使用している Flash Player のバージョンが確認できます。(現時点での最新リリースバージョンの確認もできます)

Flash Player の状況確認

Flash Player 本体のダウンロードは以下のサイトになります。

Flash Player の本体ダウンロード

*Google Chrome の場合は、Flash Player の機能がブラウザに統合されているため、Chrome 自体のアップデートを行う必要があります。

Google Chrome を更新する

*Windows 8、Windows Server 2012、Windows RT、Windows 8.1、Windows Server 2012 R2 および Windows RT 8.1 上の Internet Explorer 10 または 11 の場合は、Flash Player の機能がブラウザに統合されているため、Internet Explorer 自体のアップデートを行う必要があります。

マイクロソフト セキュリティ アドバイザリ (2755801)

【参考サイト】

CVE-2015-0359

Adobe セキュリティ情報:APSB15-06

【検証概要】

ターゲットシステムを攻撃者が用意したサイトにアクセスさせることで、Flash Player の脆弱性を利用して任意のコードを実行させます。

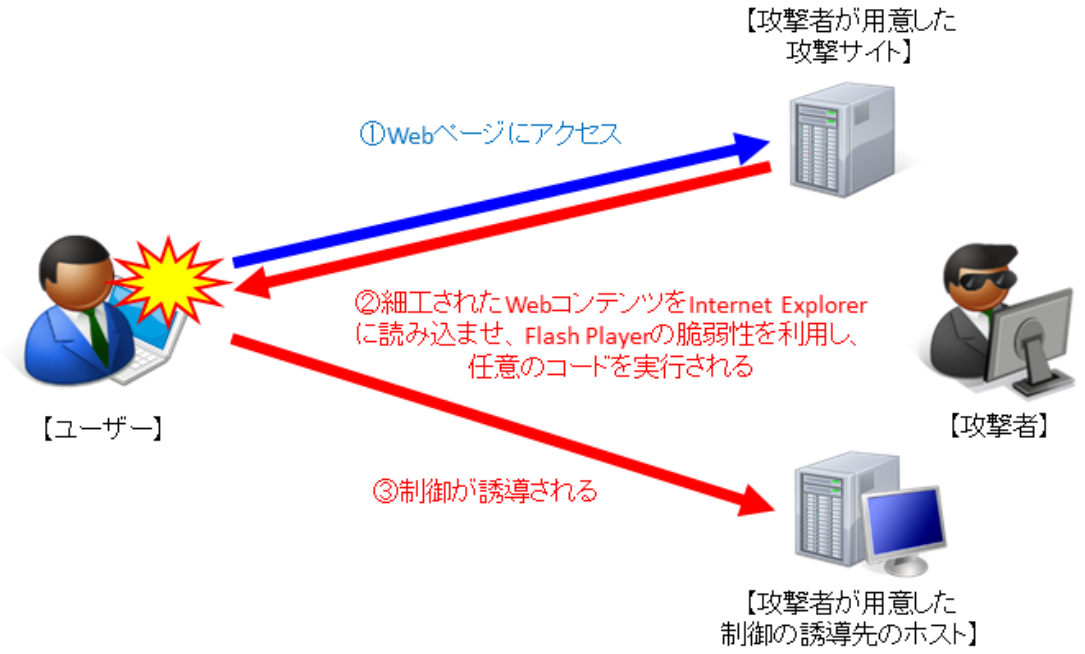
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバー、ポートへコネクションを確立させるよう誘導し、システム制御を奪取するものです。これにより、リモートからターゲットシステムが操作可能となります。

*誘導先のシステムは Linux です。

【検証ターゲットシステム】

Windows 7 SP1 日本語版 + Internet Explorer 8 + Flash Player 17.0.0.134

【検証イメージ】

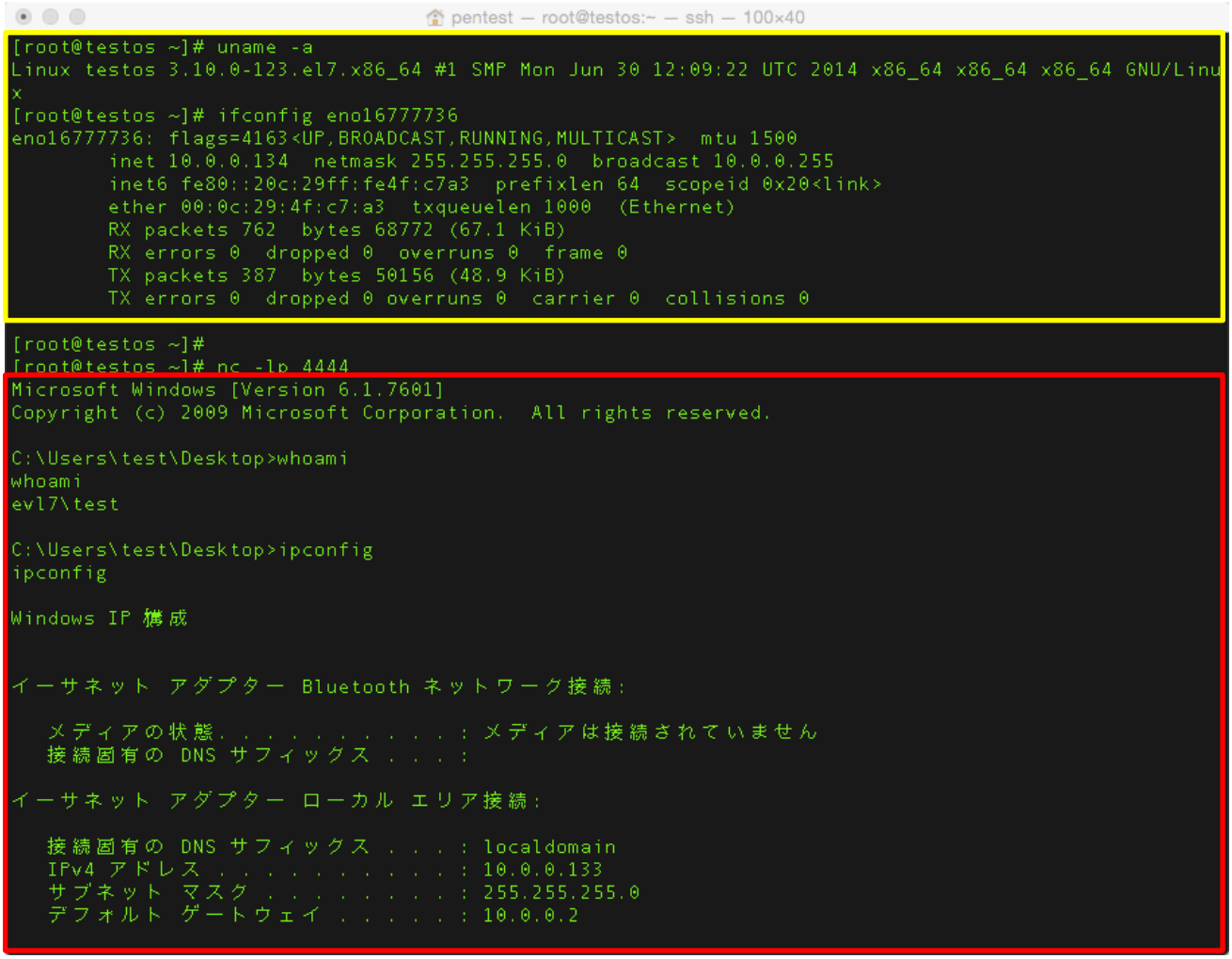


【検証結果】

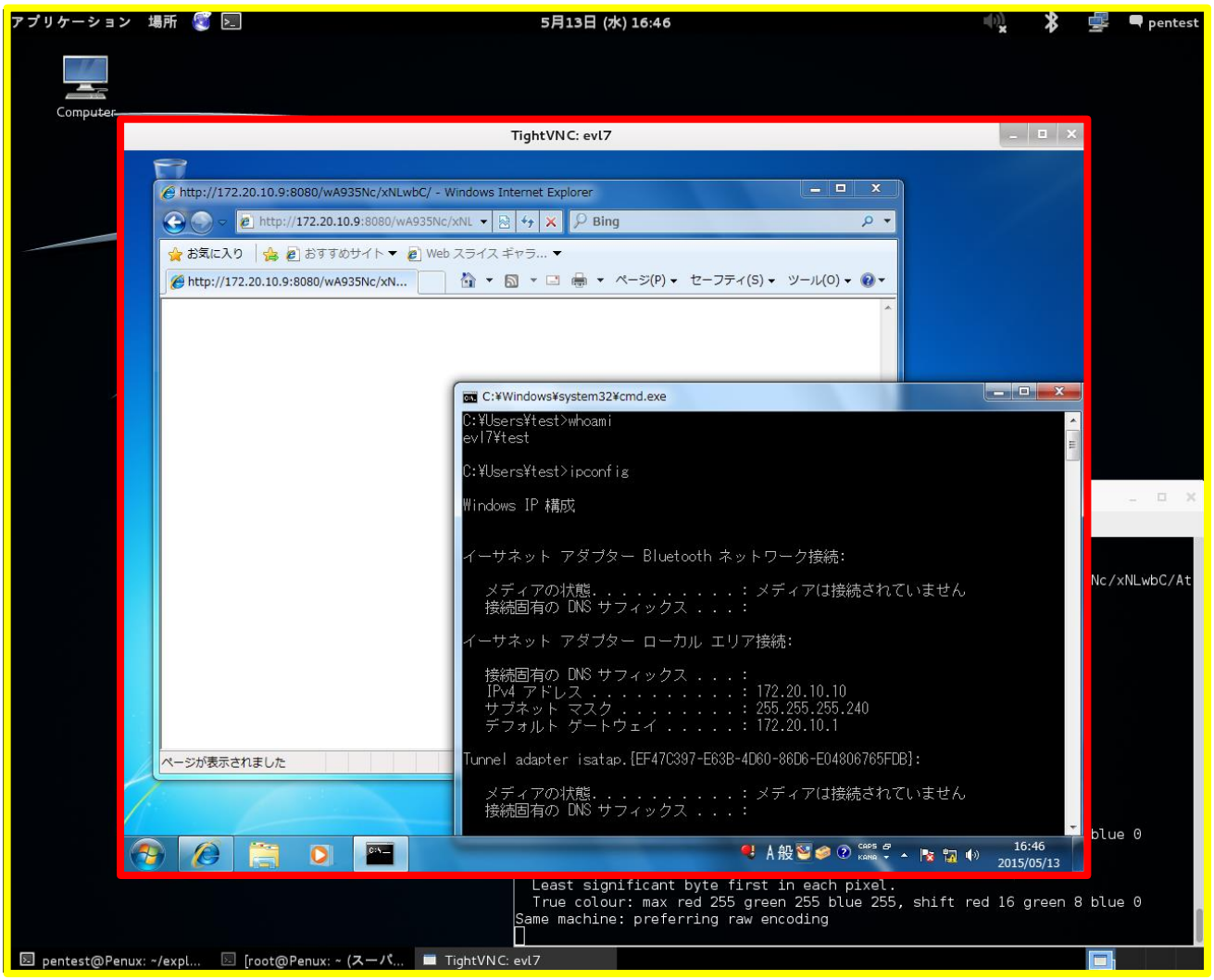
下図は、誘導先のコンピュータ（Linux）の画面です。黄線で囲まれた部分は、誘導先のコンピュータの情報です。

一方で、赤線で囲まれている部分は、ターゲットシステム（Windows 7）において、ホスト名、ユーザーの情報、IP アドレスの情報を表示する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で任意のコマンドを実行することに成功したと判断できます。



また、下図は上図とは別の任意のコードをターゲットシステムに実行させることにより、ターゲットシステムのデスクトップ画面を誘導先の Linux 上で盗み見ることに成功しています。赤線で囲まれている部分は、ターゲットシステムのデスクトップ画面です。その外側の黄線で囲まれている部分は、攻撃者のデスクトップ画面です。



【更新履歴】

2015 年 5 月 14 日 ： 初版公開

ソフトバンク・テクノロジー株式会社
〒160-0022 東京都新宿区新宿 6 丁目 27 番地 30 号
新宿イーストサイドスクエア 17 階
受付時間：平日 10:00～17:00

電話 03-6892-3154
メール sbt-ipsol@tech.softbank.co.jp
URL https://www.softbanktech.jp/