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

【更新】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-2015-5122）（APSA15-04）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-2015-5122）の攻撃コードが発見されました。

この脆弱性は、flash.display.DisplayObject クラスに解放後メモリ参照（use-after-free）の不備が存在するために起こり、Flash Player を実行するユーザーの実行権限でリモートより任意のコードを実行することが可能です。

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 を実行するユーザーの権限を奪取される危険性があります。

この脆弱性は、イタリアのセキュリティ企業、Hacking Team から流出した情報により、公になりました。流出した情報の中に、当該脆弱性を実証するコードが含まれていました。また、この脆弱性がエクスプロイトキット（=「Angler Exploit Kit」）に組み込まれ、実際の攻撃に用いられたという報告もされています。

本レポート作成（2015 年 7 月 13 日）時点において、この脆弱性を修正するプログラムはリリースされておらず、本脆弱性はゼロディの脆弱性であるという状況です。この脆弱性は、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-2015-5122）の再現性について検証を行いました。

（7 月 15 日追記）

2015 年 7 月 15 日、この脆弱性を修正するプログラムがリリースされました。

【影響を受ける可能性があるシステム】

- Windows 版および Macintosh 版の Adobe Flash Player 18.0.0.203 とそれ以前のバージョン
- Google Chrome 用 の Adobe Flash Player18.0.0.204 とそれ以前のバージョン
- Windows 版および Macintosh 版の Adobe Flash Player 継続サポートリリース 13.0.0.302 とそれ以前の 13.x バージョン
- Linux 版の Adobe Flash Player 継続サポートリリース 11.2.202.481 とそれ以前の 11.x バージョン

【対策案】

（7 月 15 日更新）

2015 年 7 月 15 日、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ました。

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。

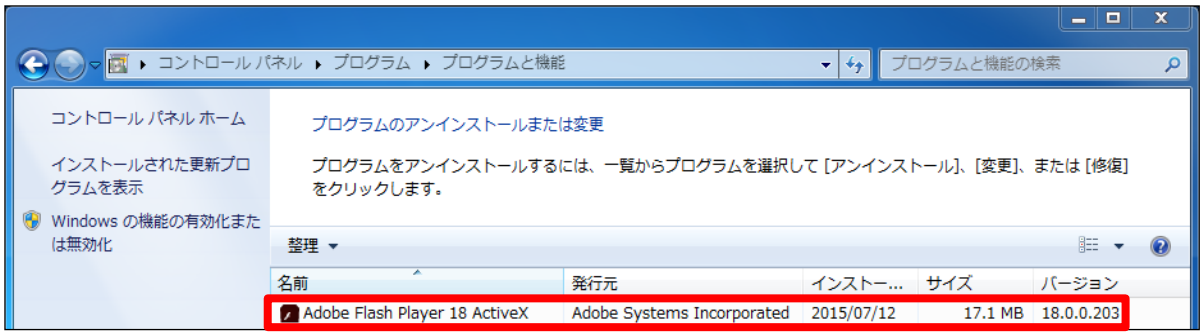
修正プログラムの適用が難しい場合、暫定策としては Adobe Flash Player を無効化/アンインストールすることが挙げられます。また、緩和策としては EMET（Enhanced Mitigation Experience Toolkit）などをインストールすることが挙げられます。しかしながら、緩和策は問題を根本的に解決するものではなく、攻撃による影響を完全に無効化できるものではないということをご留意ください。対策の実施については端末が扱う情報などを考慮し、実施範囲を業務に影響のない範囲で行っていただくことを推奨いたします。

（7 月 14 日追記）
EMET を利用することによる、主要なブラウザでの攻撃コードの実行可否について確認した結果を以下に記述します。

検証ブラウザ	EMET version 5.2
Internet Explorer 11	制限される
Firefox 39.0	**制限されない**
Chrome 43.0.2357.132m	制限される

Firefox は EMET により攻撃による影響を無効化できません。このため、Firefox を利用している場合は、Firefox のアドオンマネージャから Flash を[無効化する]の設定にしていただくことを推奨します。

【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-2015-5122
- Security updates available for Adobe Flash Player
- Security Advisory for Adobe Flash Player

【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。

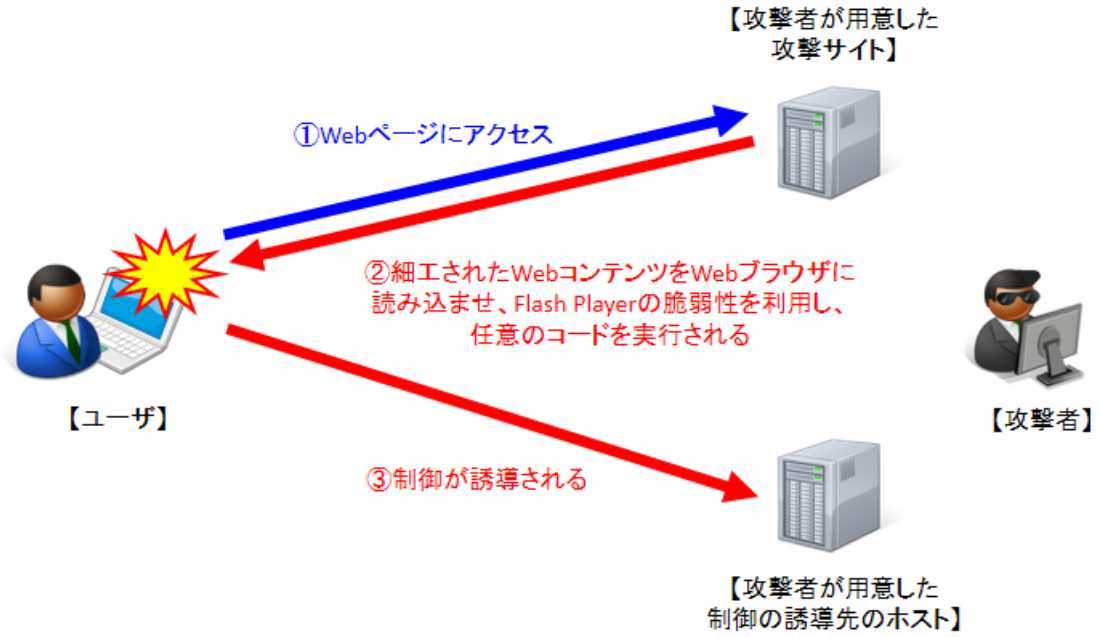
*誘導先のシステムは Linux です。

【検証ターゲットシステム】

Windows 7 SP1 日本語版 + Internet Explorer 11 + Flash Player 18.0.0.203

Windows 8.1 日本語版 + Firefox 39.0 + Flash Player 18.0.0.203

【検証イメージ】



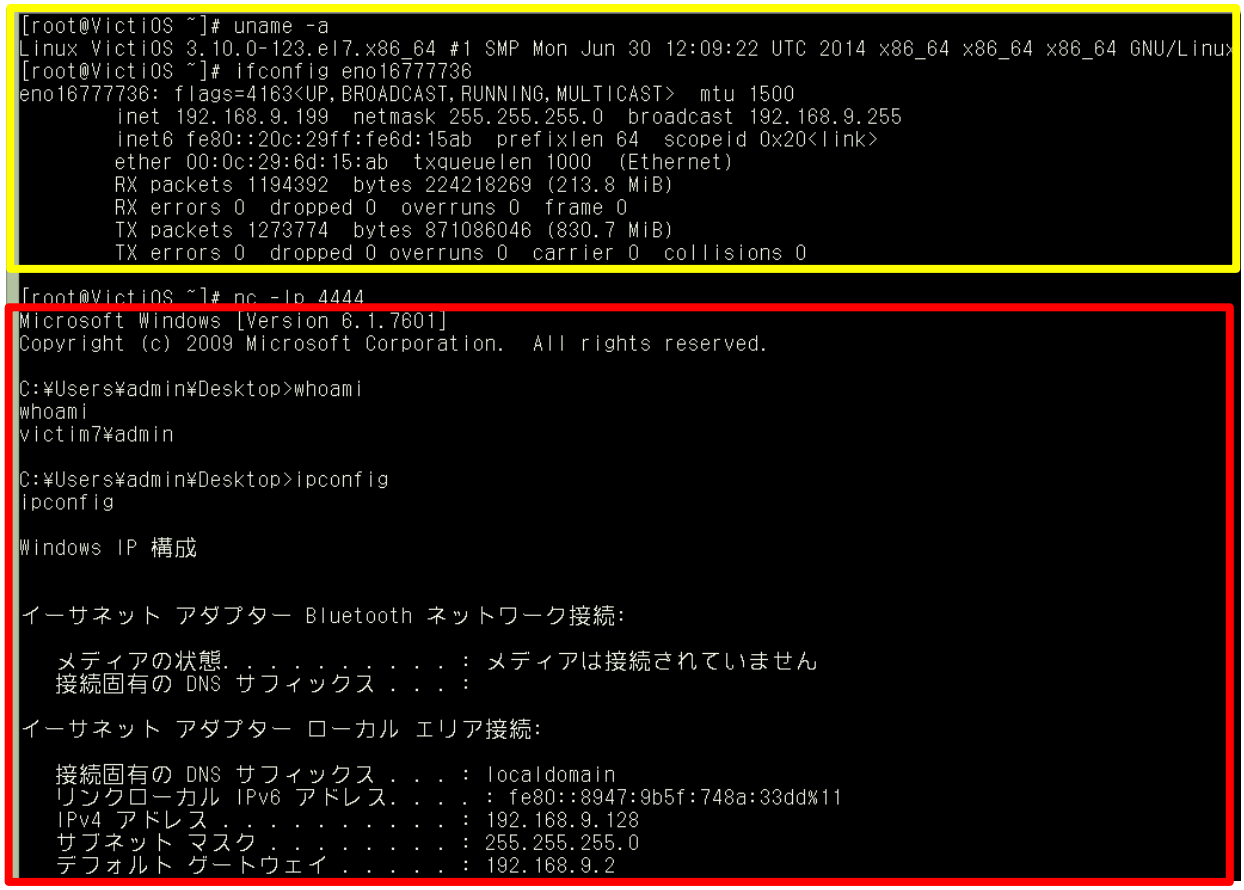
【検証結果】

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、誘導先のホストの情報です。

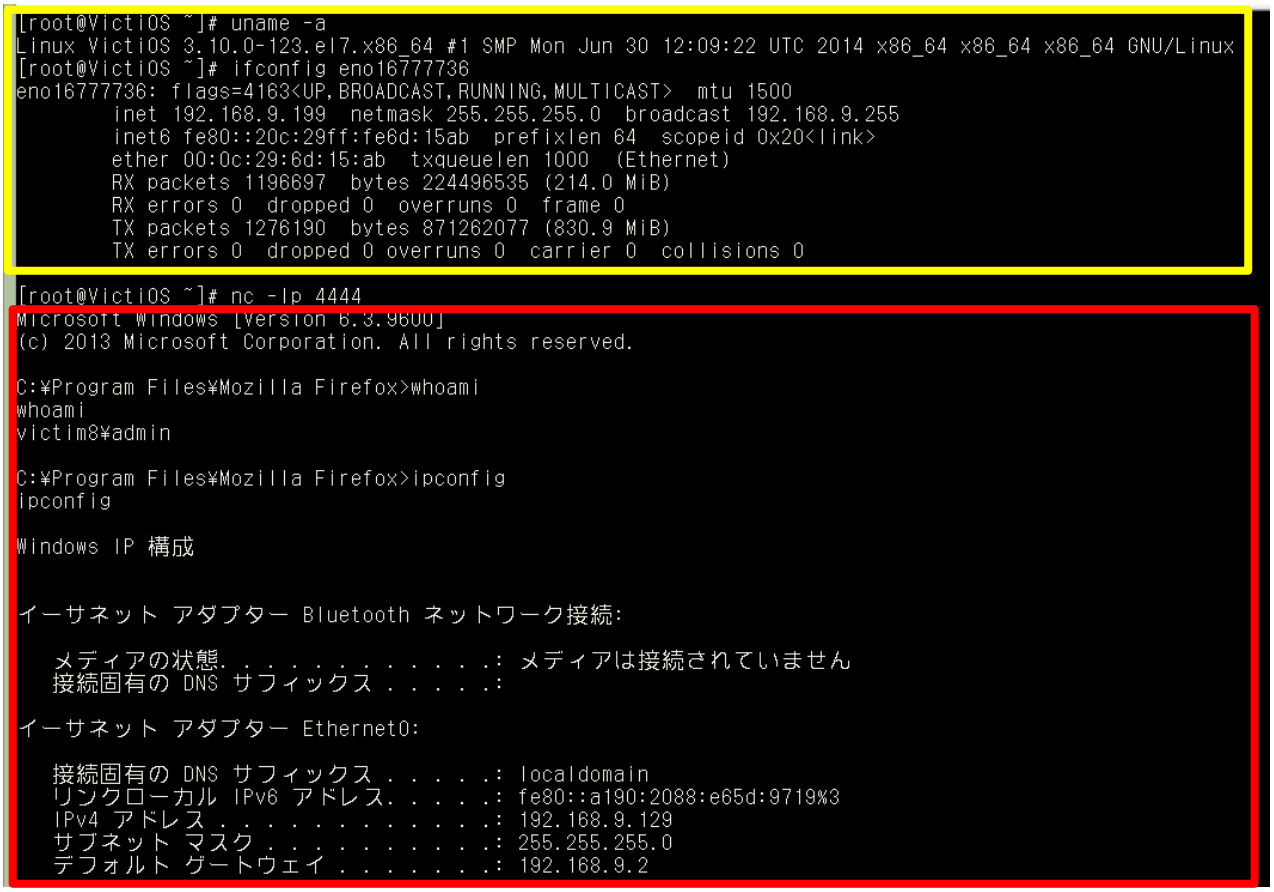
一方で、赤線で囲まれている部分は、ターゲットシステム(Windows 7 および Windows 8.1)において、ホスト名、ユーザーの情報、IP アドレスの情報を表示するコマンドを実行した結果が表示されています。

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。

Windows 7 の場合



Windows 8.1 の場合



【更新履歴】

2015 年 7 月 15 日 ： アドビ システムズ社より脆弱性を修正するプログラムがリリースされた旨を追記

2015 年 7 月 14 日 ： EMET 導入による Internet Explorer, Firefox, Chrome での検証結果を追記

2015 年 7 月 13 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/