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 PCRE エンジンのコンパイル処理の脆弱性により、リモートから任意のコードが実行可能な脆弱性（CVE-2015-0318）(APSB15-04)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-2015-0318）が発見されました。この脆弱性は、PCRE エンジンのコンパイル処理に不備が存在するため、エスケープシーケンスの処理に問題が発生することにより起こります。

これにより、攻撃者は、任意のコードを実行、メモリ破損や、サービス運用妨害をすることが可能です。

攻撃者は、細工された Web サイトに利用者を訪問させることにより、リモートからブラウザを実行する利用者のユーザ権限にて任意のコードを実行できる可能性があります。方法としては、リンクを記述した電子メールなどでメッセージを送信し、攻撃対象ユーザを細工した Web サイトへ誘導したり、日常的に攻撃対象ユーザがアクセスするサイトを改ざんし、攻撃を行うサイトに作り替えるなどしてアクセスしてきた際に本脆弱性を利用し、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ます。

今回、この脆弱性（CVE-2015-0318）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】

・アドビシステムズ

- Adobe Flash Player デスクトップランタイム 16.0.0.305 未満 (Windows/Macintosh)
- Adobe Flash Player 継続サポートリリース 13.0.0.269 未満 (Windows/Macintosh)
- Adobe Flash Player 11.2.202.442 未満 (Linux)
- Adobe Flash Player 16.0.0.305 未満 (Windows/Macintosh/Linux 版の Chrome)
- Adobe Flash Player 16.0.0.305 未満 (Internet Explorer 10/11)

・Google Chrome

- Google Chrome 40.0.2214.115 未満 (Windows/Macintosh/Linux)

・Microsoft Internet Explorer

- Microsoft Internet Explorer 10 (Windows 8/Windows Server 2012/Windows RT)
- Microsoft Internet Explorer 11 (Windows 8.1/Windows Server 2012 R2/Windows RT 8.1)

【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。

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)

*本調査レポートの脆弱性の他に、3月の更新にて修正された、CVE-2015-0336 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。(2015/3/24 時点)
(参考:Adobe セキュリティ情報:APSB15-05)

【参考サイト】
- CVE-2015-0318
- Adobe セキュリティ情報:APSB15-04
- JVNDB-2015-001330 - JVN iPedia - 脆弱性対策情報データベース: JVNDB-2015-001330

【検証概要】

ターゲットシステムのユーザを、Internet Explorer にて、あらかじめ細工した Web サイトにアクセスさせます。これにより任意のコードが実行されます。

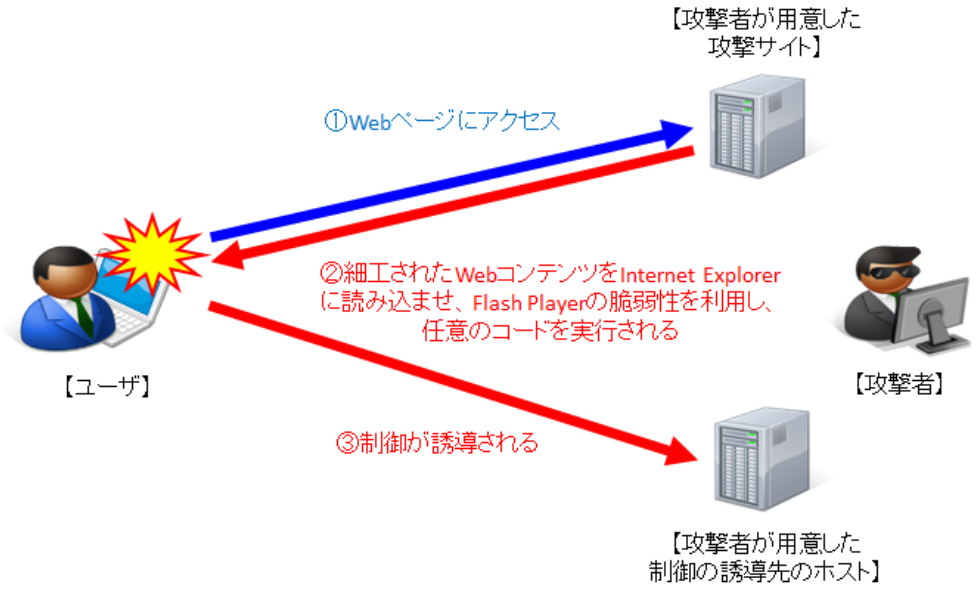
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバー、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。これにより、リモートからターゲットシステムが操作可能となります。

＊ 誘導先のシステムは Mac OS X 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 16.0.0.235

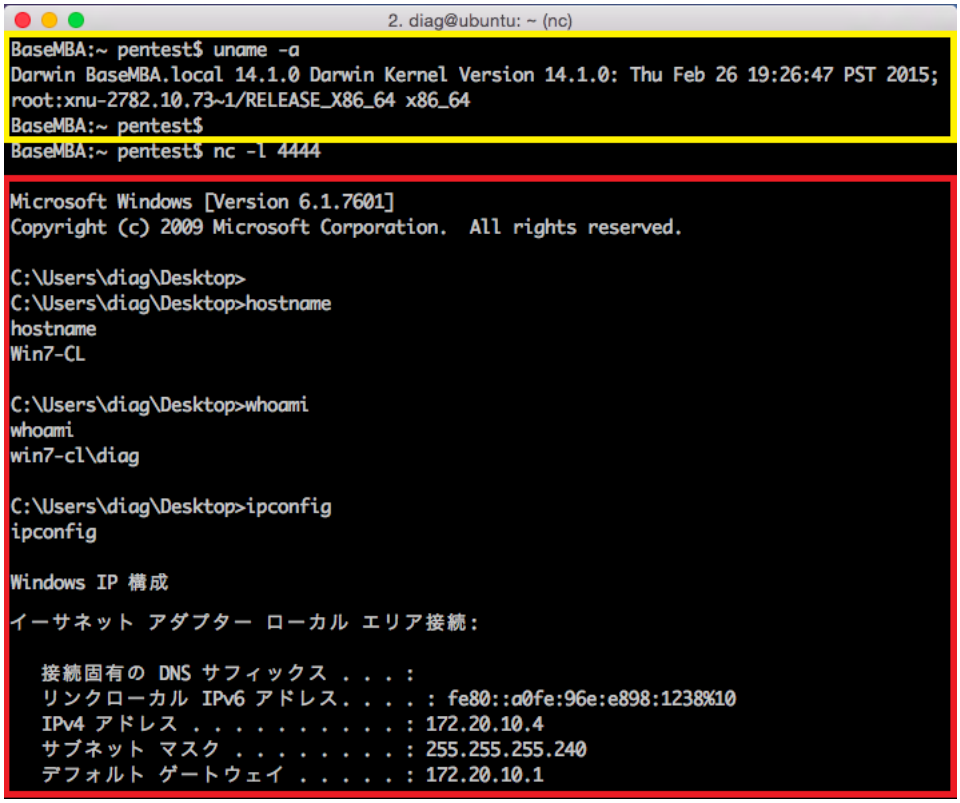
【検証イメージ】



【検証結果】

下図は、誘導先のコンピュータ(Mac OS X)の画面です。黄線で囲まれている部分は、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(Windows7)において、ホスト名、ユーザの情報、IPアドレス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。



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/