2015 年 7 月 3 日
株式会社セキュアソフト

Sniper IPS による対策：Adobe Flash Player の脆弱性（CVE-2015-3113）に対応

1. 概要

アドビシステムズ社の Adobe Flash Player に任意コードの実行可能な脆弱性が見つかり、これを利用する標的型サイバー攻撃が確認されました。 この攻撃を受けた場合には、アプリケーションプログラムが異常終了したり、攻撃者によって PC が遠隔操作されるなど、様々な被害が発生する可能性があります。Sniper IPS ではこの脆弱性に対する攻撃を検知・防御する対応を追加しております。

2. 攻撃方法

CVE-2015-3113 の脆弱性は、細工された Flash Player 用の動画ファイル（FLV ファイル）を構文解析する際に発生します。攻撃者はターゲットユーザが不正な FLV ファイルを閲覧するように様々な手法で標的型サイバー攻撃を行います。攻撃者は不正な FLV ファイルを閲覧したターゲットユーザ端末のセキュリティ対策を迂回する為に、高度な技術を利用してユーザ端末（PC）のメモリ全体をアクセスします。又、バッファーオーバーフローを発生させてターゲットユーザのコンテキストで任意のコードを実行させます。攻撃に成功すると、攻撃者は外部からターゲットユーザ端末（PC）を遠隔操作します。

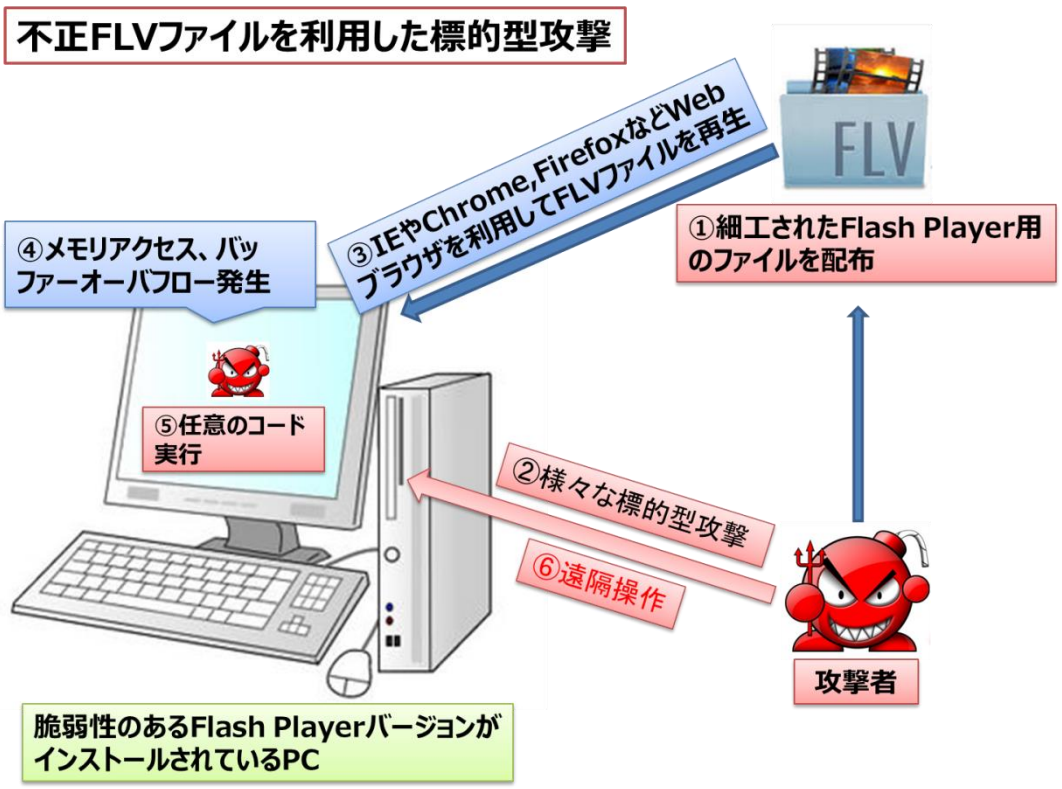

図 1　CVE-2015-3113 脆弱性を利用した攻撃の流れ

3. 脆弱システム

以下の Adobe Flash Player が脆弱な対象となります。詳細はアドビシステムズ社のセキュリティ情報を確認してください。

- Windows 版 と Macintosh 版 の Adobe Flash Player 18.0.0.161 と以前のバージョン
- Windows 版 と Macintosh 版 の Adobe Flash Player の継続サポートリリースバージョン 13.0.0.292 と以前の 13.x バージョン
- Linux 版の Adobe Flash Player 11.2.202.466 とそれ以前の 11.x バージョン

4. 対応方法

端末ならびにネットワークシステムでの対策が可能です。早急に対策を実施する必要があります。

① 端末での対策

端末（PC）にインストールされている Adobe Flash Player や Internet Explorer, Google Chrome などのウェブブラウザを最新版に更新します。

② ネットワークシステムでの対策（Sniper IPS による対策）

ネットワークシステム上にある様々セキュリティ対策製品を利用して攻撃を防御できます。一般的な IPS では今回の攻撃に対する最新のシグネチャが提供されていますので、確認されることをおすすめします。

Sniper IPS は該当の脆弱性に対応するための緊急シグネチャを 6 月 25 日にリリースしております。以下のシグネチャを利用して検知・防御が可能となります。

表 1 Adobe Flash Player の脆弱性に対応するシグネチャ情報

攻撃コード	**3141**
攻撃名	**Adobe Flash Player malformed .flv Remote Code Execution**
攻撃パターン	**パターンブロック**

以上