2015 年 7 月 17 日
株式会社セキュアソフト

Sniper IPS による対策：Adobe Acrobat および Reader の脆弱性

1. 概要

最近、アドビシステムズ社が提供している Adobe Acrobat および Reader プログラムから多くの脆弱性が発生している状況です。この脆弱性に対してセキュリティアップデートを実施しない場合には、攻撃者から任意のコードの実行（遠隔操作）や、運用妨害（メモリ破壊）などの危険性があります。

2. 攻撃説明

Adobe Acrobat および Reader の脆弱性については、多数報告がありますが CVE-2015 -3057 の脆弱性に関連する攻撃方法について説明いたします。

CVE-2015-3057 脆弱性は、初期化されていないポインター値へ接続するため発生します。

以下のような流れで攻撃が行われます。

① 脆弱性を利用した悪意のある PDF 文書ファイル（this.closeDoc(true)スクリプト）を作成します。
② 攻撃者は、悪意のあるファイルを閲覧するように誘導します。
③ 誘導によって悪意のある PDF 文書を読む際に①のスクリプトが実行されます。
④ ①のスクリプトが実行されると PDF 文書のポインター値を削除して初期化されていないポインターが発生します。
⑤ 攻撃者は④で解放されたメモリを利用します。
⑥ 攻撃に成功すると、攻撃対象端末（パソコン）もしくは対象プロセスで選択した全てのコマンドが実行できる不正行為が可能となります。

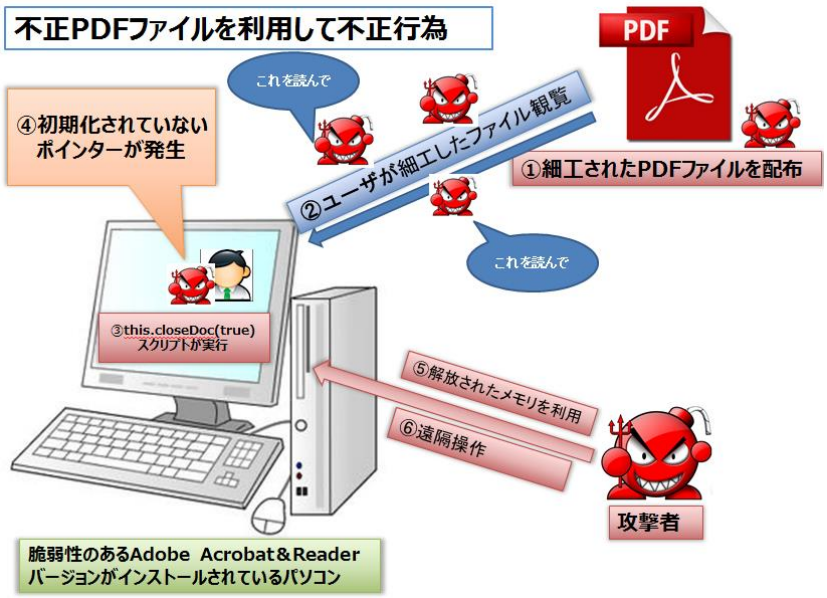

図 1 CVE-2015-3057 脆弱性を利用した攻撃の流れ

3. 対象バージョン

アップデートが対象となる Acrobat および Reader のバージョンは以下となります。

No	対象バージョン
1	Acrobat XI (11.0.11) およびそれ以前のバージョン（Windows 版,Macintosh 版)
2	Acrobat X (10.1.14) およびそれ以前のバージョン（Windows 版,Macintosh 版)
3	Reader XI (11.0.11) およびそれ以前のバージョン（Windows 版,Macintosh 版)
4	Reader X （10.1.14) およびそれ以前のバージョン（Windows 版,Macintosh 版)

4. 対応方法

① 端末での対策

端末（パソコン）にインストールされている Adobe Acrobat および Reader を最新版に更新します。

https://helpx.adobe.com/security/products/reader/apsb15-10.html

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な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 では今回の攻撃を含めた複数の Adobe Acrobat および Reader の脆弱性に対する最新のシグネチャがリリースされています。また、Sniper IPS では 7 月 15 日に以下のシグネチャが提供されていますのでご確認ください。

Adobe Acrobat および Reader の脆弱性に対応するシグネチャ一覧

攻撃コード	攻撃名	対象 CVE-ID
3153	Adobe Acrobat & Reader privileged JavaScript Execution	CVE-2014-8448
3154	Adobe Reader JBIG2 Row Out of Bounds Memory Corruption	CVE-2014-8446
3155	Adobe Acrobat & Reader ANTrustPropgateAll privilege	CVE-2014-8451
3156	Adobe Acrobat & Reader Close Page Action Use-After-Free	CVE-2015-3053
3157	Adobe Acrobat and Reader WillSave Document Action Use-After-Free	CVE-2015-3054
3158	Adobe Acrobat & Reader Uninitialized Pointer RCE	CVE-2015-3057
3161	Adobe Acrobat Reader UTF-16 string BoF	CVE-2014-0524
3162	Adobe Acrobat Reader Decoding DCT Memory Corruption	CVE-2014-0526
3163	Adobe Acrobat Reader embedded PRC stream Remote Code Execution	CVE-2014-0522

以上