NTTデータ・セキュリティ株式会社

Adobe Reader、及び、Acrobat の Doc.media.newPlayer の脆弱性(CVE-2009-4324)に関する検証レポート

2009/12/16
2010/01/13(更新)
診断ビジネス部
辻　伸弘
松田　和之

【概要】

Adobe Reader、及び、Acrobat の Doc.media.newPlayer メソッドの処理に脆弱性が存在することが発見されました。
Doc.media.newPlayer メソッドは、Adobe Reader、及び、Acrobat の JavaScript で利用されるメソッドであり、解放したメモリ領域を参照する脆弱性（Use After Free）が存在します。
攻撃者は、メモリ中に任意のコードをコピーし、Doc.media.newPlayer メソッドの脆弱性を利用してメモリ領域を参照させ、任意のコードを実行させます。

この脆弱性により、Web ページの閲覧、HTML 形式の電子メールの表示、または、電子メールの添付ファイルなどの経路から細工された PDF ファイルを閲覧した場合に、そのローカルユーザと同じ権限が奪取される恐れがあります。
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、Adobe Reader、及び、Acrobat の脆弱性（CVE-2009-4324）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、Acrobat のバージョン 9.2 以下のバージョン

【対策案】

このレポート作成現在（2009 年 12 月 16 日）、修正プログラムはリリースされておりません。
なお、修正プログラムは、2010 年 1 月 12 日にリリースされる予定です。

2010 年 1 月 13 日追記：

Adobe 社から、修正されたバージョン「9.3」、「8.2」がリリースされています。
修正されたバージョンへアップデートしたシステムに対して再度検証を行った結果、脆弱性の再現ができないことが確認されました。

充分な検証の後、運用に支障をきたさないことをご確認の上、修正されたバージョン「9.3」、または、「8.2」へアップデートすることが推奨されます。
http://get.adobe.com/jp/reader/

また、本脆弱性は JavaScript 処理の脆弱性であり、Adobe Reader、及び、Acrobat において JavaScript を無効にすることも対策となります。
JavaScript 処理における脆弱性は、本脆弱性以外に過去複数報告されているものであり、Adobe Reader、及び、Acrobat において JavaScript 処理が、運用上必要かどうか確認し、不要であれば、無効にすることが推奨されます。

なお、JavaScript 処理の無効化等の「環境設定」は、アップデートした場合には継承されますが、再インストールした場合にはデフォルト値に戻ります。そのため、再インストールした場合は、JavaScript 処理の設定を再度、確認することが推奨されます。

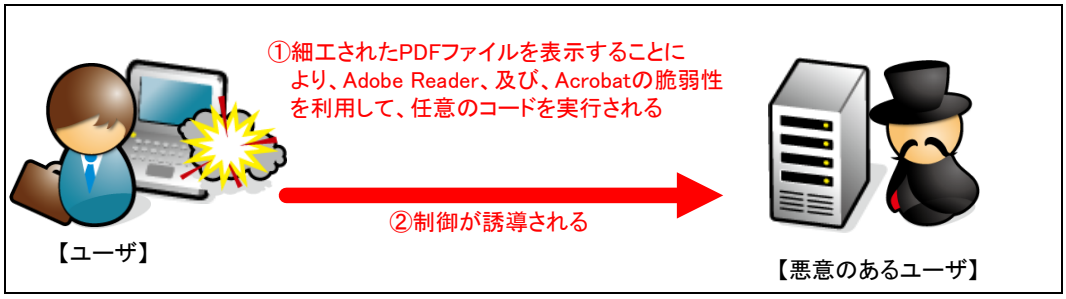
Adobe 社のセキュリティアドバイザリにて、Adobe Reader、Acrobat のバージョン 9.2、または、8.1.7 の場合の脆弱性の対策方法が紹介されています。
Security Advisory for Adobe Reader and Acrobat
http://www.adobe.com/support/security/advisories/apsa09-07.html

【参考サイト】

CVE-2009-4324
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4324

NTTデータ・セキュリティ株式会社

【検証イメージ】



【検証ターゲットシステム】

Adobe Reader 9.0.0 がインストールされた Windows XP

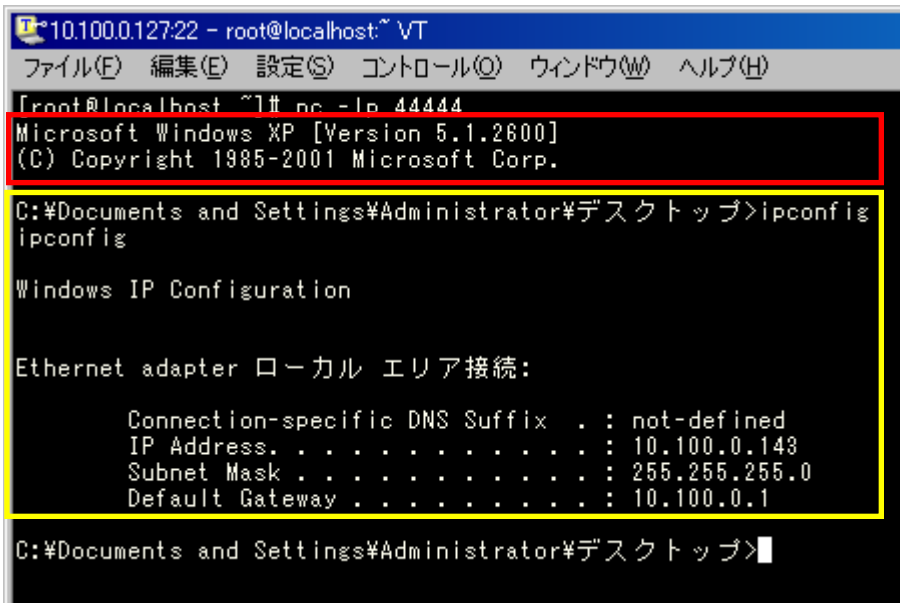
【検証概要】

ターゲットシステム上で、細工した PDF ファイルを表示す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を操作可能となります。
＊ 誘導先のシステムは CentOS 4.4 です。

【検証結果】

下図の赤線で囲まれている部分が示すように、誘導先のコンピュータ（CentOS）のコマンドプロンプト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。
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



＊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。

NTTデータ・セキュリティ株式会社

【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/