NTTデータ先端技術株式会社

Windows Packager 設定における任意のコードを実行可能な脆弱性 (MS12-005)(CVE-2012-0013)に関する検証レポート

2012/1/17
NTT データ先端技術株式会社
辻 伸弘
泉田 幸宏

【概要】

ClickOnce アプリケーションを含む細工された Microsoft Office ファイルをユーザが開いた場合に、任意のコードが実行される脆弱性が発見されました。
ClickOnce とは、.NET Framework 2.0 以降から利用可能となったリンクをクリックするだけでアプリケーションの実行を行えるというものです。
本脆弱性は、Click Once アプリケーションのファイルの種類が、Windows Packager の安全ではないファイルの種類のリストに含まれていないことにより発生します。

この脆弱性により、細工されたファイルを閲覧させることで、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。

今回、この Windows の脆弱性（MS12-005）（CVE-2012-0013）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】

-Windows XP Service Pack 3
-Windows XP Professional x64 Edition Service Pack 2
-Windows Server 2003 Service Pack 2
-Windows Server 2003 x64 Edition Service Pack 2
-Windows Server 2003 with SP2 for Itanium-based Systems
-Windows Vista Service Pack 2
-Windows Vista x64 Edition Service Pack 2
-Windows Server 2008 for 32-bit Systems Service Pack 2**
-Windows Server 2008 for x64-based Systems Service Pack 2**
-Windows Server 2008 for Itanium-based Systems Service Pack 2
-Windows 7 for 32-bit Systems および Windows 7 for 32-bit Systems Service Pack 1
-Windows 7 for x64-based Systems および Windows 7 for x64-based Systems Service Pack 1
-Windows Server 2008 R2 for x64-based Systems および Windows Server 2008 R2 for x64-based Systems Service Pack 1**
-Windows Server 2008 R2 for Itanium-based Systems および Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
**Server Core インストールでは影響を受けません。

【対策案】

Microsoft 社より、この脆弱性を修正するプログラム（MS12-005）がリリースされています。
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いたします。

【参考サイト】

CVE-2012-0013
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0013

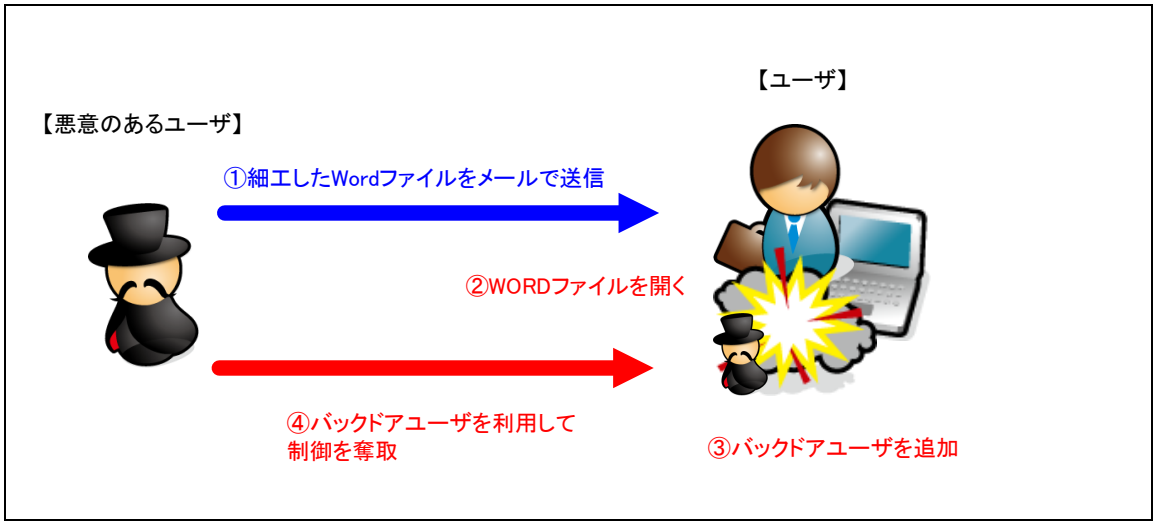
マイクロソフト セキュリティ情報 MS12-005 - 重要
Microsoft Windows の脆弱性により、リモートでコードが実行される (2584146)
http://technet.microsoft.com/ja-jp/security/bulletin/ms12-005

JVNDB-2012-001048
複数の Microsoft Windows 製品の Windows Packager 設定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/2012/JVNDB-2012-001048.html

NTTデータ先端技術株式会社

NTTデータ先端技術株式会社

【検証イメージ】



【検証ターゲットシステム】

Windows Vista

※確認用に Windows 7

【検証概要】

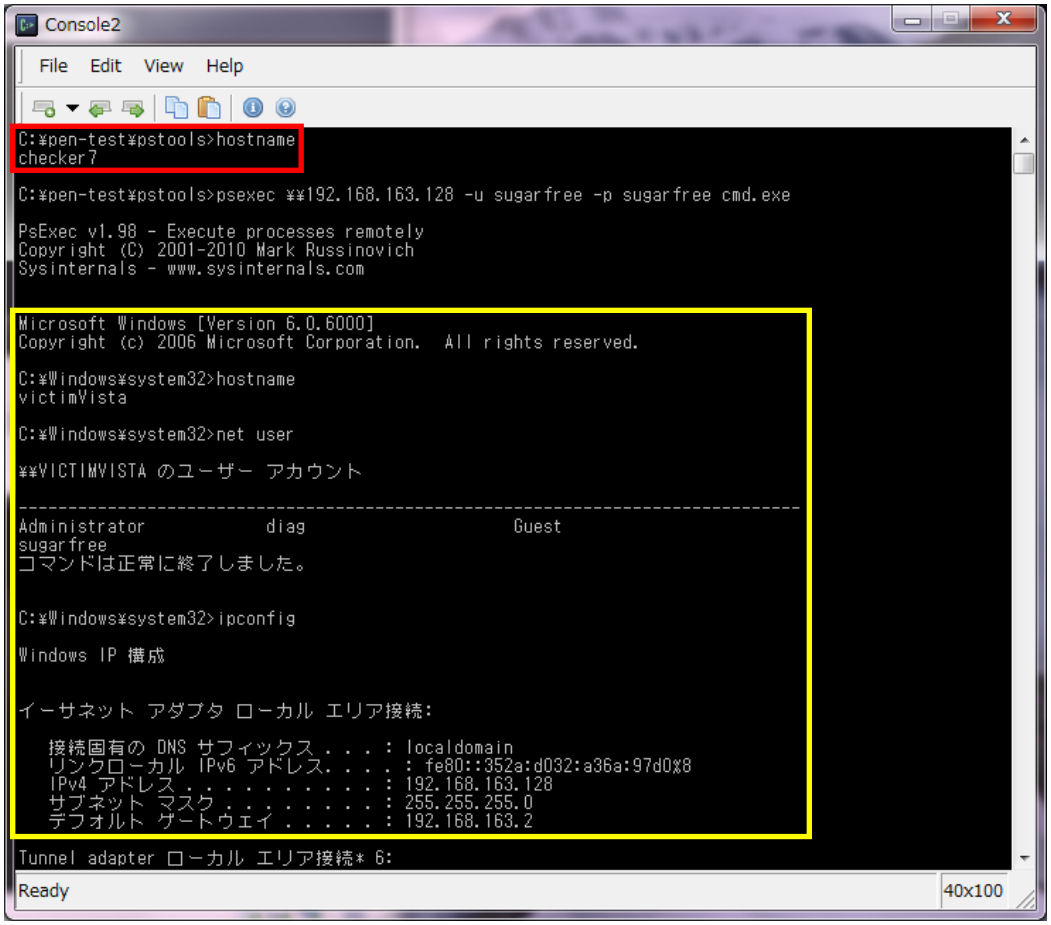
ターゲットシステムで細工された WORD ファイルを開かせることで任意のコードを実行させます。
今回の検証は、ターゲットシステム上にバックドア用のユーザ（sugarfree）を追加し、そのユーザを利用してシステム制御を奪取するというものです。
これにより、リモートからターゲットシステムの操作を奪取可能となります。

NTTデータ先端技術株式会社

【検証結果】

下図の赤線で囲まれている部分は、確認用のコンピュータ「cheker7（Windows 7)」上でのコマンド実行結果を示しています。
黄線で囲まれている部分は、ターゲットシステムのホスト名、ユーザアカウント情報、ネットワークアドレス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。

【お問合せ先】

NTT データ先端技術株式会社
セキュリティ事業部　営業担当　営業企画グループ
TEL：03-5425-1954
http://security.intellilink.co.jp/