NTTデータ・セキュリティ株式会社

Windows シェルにおけるショートカットファイル処理の脆弱性（CVE-2010-2568）に関する検証レポート

2010/7/20
NTT データ・セキュリティ株式会社
辻 伸弘

【概要】

Windows シェルのショートカットファイル処理に脆弱性が存在します。
この脆弱性は細工されたショートカットファイル「.lnk」を Windows のエクスプローラで表示させることにより任意のコードが実行されるというものです。
悪用されるケースとしては、USB メモリなどのリムーバブルメディア経由とリモートファイル共有経由などが挙げられます。前者に関しては、リムーバブルメディア内に細工したショートカットファイルが存在し、AutoRun 機能が有効にされていた場合、リムーバブルメディア接続後、自動で任意のコードを実行するという攻撃方法が考えられます。この機能については、既に実装しているマルウェアが発見されています。
また、後者に関しては、ブラウザによる閲覧をトリガとして不正な WebDav サーバへと誘導し、細工したショートカットファイルを閲覧させるという攻撃方法が考えられます。

この脆弱性により、リムーバブルメディアや細工された 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-2010-2568）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 1 および Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 1 および Windows Vista x64 Edition Service Pack 2
- Windows Server 2008 for 32-bit Systems および Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for x64-based Systems および Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for Itanium-based Systems および Windows Server 2008 for Itanium-based Systems Service Pack 2
- Windows 7 for 32-bit Systems
- Windows 7 for x64-based Systems
- Windows Server 2008 R2 for x64-based Systems
- Windows Server 2008 R2 for Itanium-based Systems

【対策案】

このレポート作成現在（2010 年 7 月 20 日）修正プログラムはリリースされていません。
Microsoft 社は以下の回避策を提示しています。

- ショートカット用アイコンの表示を無効にする
- WebClient サービスを無効にする

詳細および回避策の影響については
「マイクロソフト セキュリティ アドバイザリ (2286198)」の「回避策」を参照ください。
http://www.microsoft.com/japan/technet/security/advisory/2286198.mspx

NTTデータ・セキュリティ株式会社

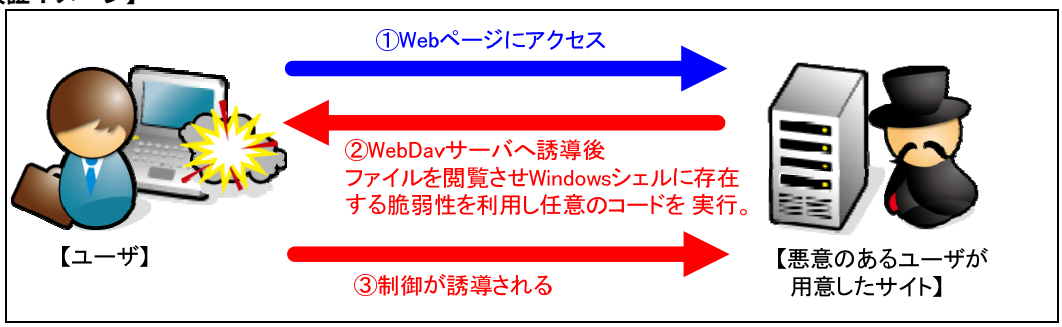
【参考サイト】

マイクロソフト セキュリティ アドバイザリ (2286198)
Windows シェルの脆弱性により、リモートでコードが実行される
http://www.microsoft.com/japan/technet/security/advisory/2286198.mspx

JVNVU#940193 Microsoft Windows のショートカットファイルの処理に脆弱性
http://jvn.jp/cert/JVNVU940193/index.html

CVE-2010-2568
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568

【検証イメージ】



【検証ターゲットシステム】

Windows XP SP3（2010 年 7 月 20 日時点にリリースされているすべての修正プログラムを適用済み）

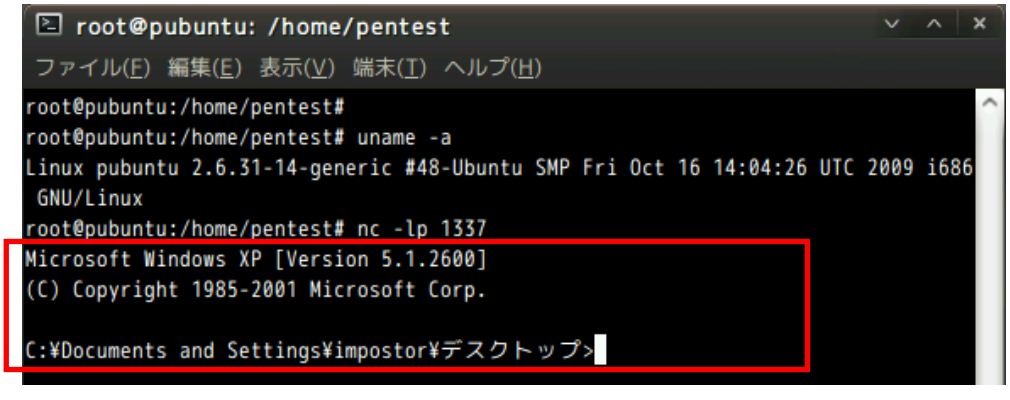
【検証概要】

ターゲットシステムに、Web ブラウザを通じて、細工したサイト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 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。
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



NTTデータ・セキュリティ株式会社

＊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
企画部　広報グループ
TEL：03-5425-1954
http://www.nttdata-sec.co.jp/