

Windows アニメーション カーソル処理の脆弱性に関するレポート

2007/04/03

NTT データ・セキュリティ株式会社
辻 伸弘

【概要】

Microsoft 社の Windows のアニメーション カーソル (.ani) ファイルを処理する方法に脆弱性が存在することが発見されました。この脆弱性により、巧妙に細工された Web ページの閲覧、HTML 電子メールを表示すると、ローカルユーザーと同じ権限の制御が奪取される恐れがあります。想定される被害としては、ユーザ権限での情報の取得、改ざん、または、ワームやスパイウェアなどの悪意の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。また、この脆弱性を利用した攻撃が行われていることが確認されております。

今回、この脆弱性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】

Microsoft Windows 2000 Service Pack 4
Microsoft Windows XP Service Pack 2
Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium)
Microsoft Windows XP Professional x64 Edition
Microsoft Windows Server 2003
Microsoft Windows Server 2003 for Itanium-based Systems
Microsoft Windows Server 2003 Service Pack 1
Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
Microsoft Windows Server 2003 x64 Edition
Microsoft Windows Vista

【検証ターゲットシステム】

Windows Vista
Windows XP Professional + Service Pack2(レポート作成時点フルパッチを適用)

【検証アタックシステム】

Windows XP Professional + Service Pack2(レポート作成時点フルパッチを適用)

【検証概要】

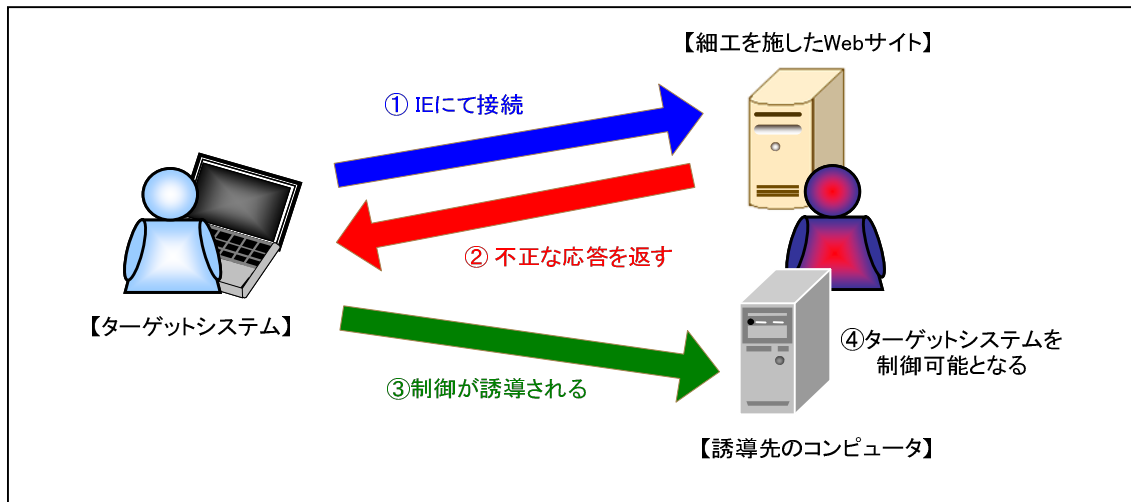
ターゲットシステム上の Internet Explorer (IE) に、細工を施した Web ページを閲覧させることで任意のコードを実行させます。

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。

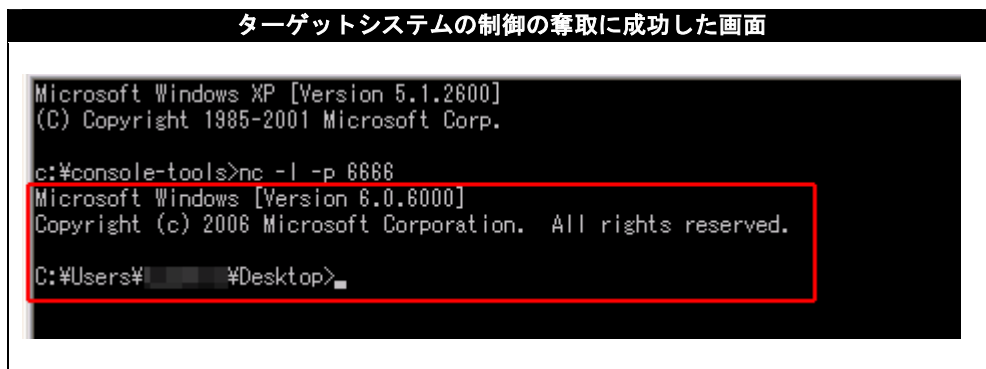
* 誘導先のシステムは Windows XP Pro + Service Pack2 です。

【検証イメージ】



【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（OS：Windows XP）のコマンドプロンプト上にターゲットシステム（Windows Vista）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。（下図は、【検証イメージ】中の④の状態に当たります。）



【対策案】

米国時間 2007/04/03（日本時間では 2007/04/04 未明の見込み）に Microsoft 社より提供されるプログラムを適用することを推奨いたします。
修正プログラムのリリース、適用までは、怪しいサイトやメールの閲覧を行わない、または、Internet Explorer (IE)、Outlook Express (OE) などの影響を受ける製品の代替を使用することが推奨されます。

【参考サイト】

マイクロソフト セキュリティ アドバイザリ (935423)
<http://www.microsoft.com/japan/technet/security/advisory/935423.msp>

* 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/>