NTTデータ・セキュリティ株式会社

Kodak Image Viewer の脆弱性に関する検証レポート

2007/11/13
NTT データ・セキュリティ株式会社
辻 伸弘
松田 和之

【概要】

Microsoft 社の Windows に搭載されている Kodak Image Viewer が画像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、細工された画像ファイルを含む Web ページの閲覧、HTML 電子メールの表示、または、電子メールの添付を開いた場合に、ローカルユーザ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、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、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】

Windows 2000 Service Pack 4
Windows XP Service Pack 2 (*1)
Windows Server 2003 Service Pack 1 および Windows Server 2003 Service Pack 2 (*1)

(*1)Windows 2000 からアップグレードしたもののみ対象であり、Windows XP/Server 2003 をクリーンインストールした場合、Kodak Image Viewer は OS に含まれないため、影響を受けません。

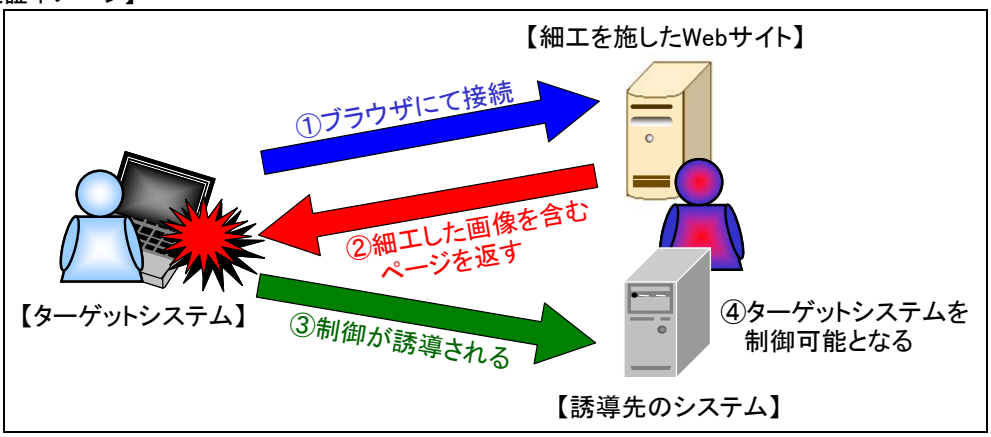
【検証ターゲットシステム】

Windows 2000 Advanced Server Service Pack 4 (日本語版)

【検証概要】

ターゲットシステムに、細工した画像ファイルを含む 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 Professional Service Pack 2 です。*

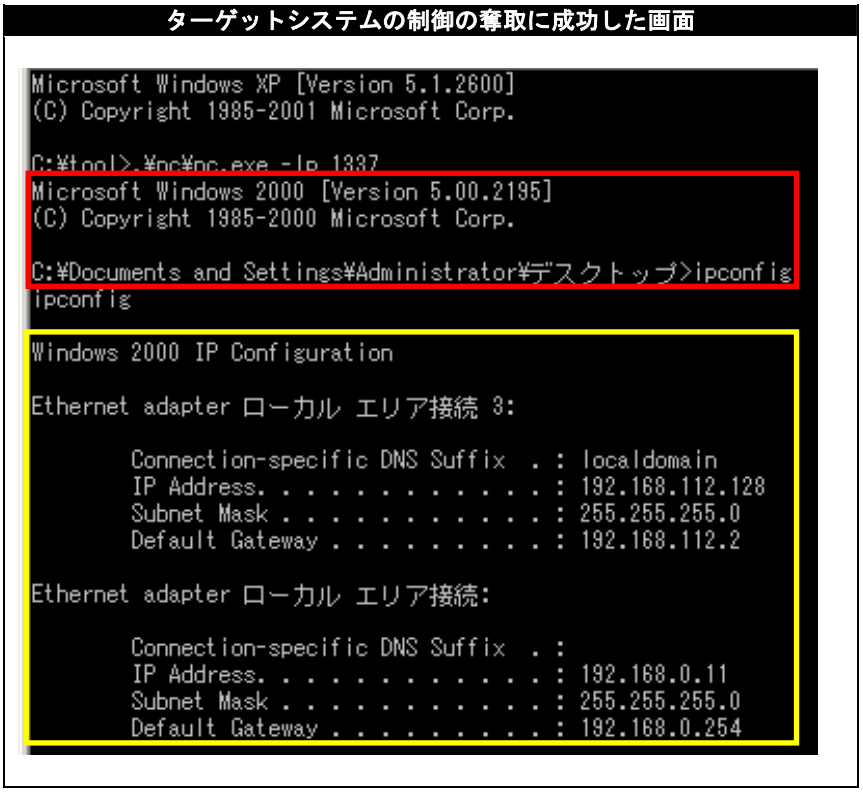
【検証イメージ】



【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（Windows XP）のコマンドプロンプト上にターゲットシステム（Windows 2000）のプロンプトが表示されております。
黄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おります。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



【対策案】

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、修正プログラムの適用を行ってください。

【参考サイト】

Kodak Image Viewer の脆弱性により、リモートでコードが実行される (923810)
http://www.microsoft.com/japan/technet/security/bulletin/ms07-055.mspx

＊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/