NTTデータ・セキュリティ株式会社

IE のポインタ参照処理の脆弱性(CVE-2010-0249)に関する検証レポート

2010/1/18
2010/1/22(更新)
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 Internet Explorer （以下 IE）の脆弱性 （CVE-2010-0249）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 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。
また、この脆弱性を利用した攻撃事例はすでに存在し、有名企業での被害が発生したとの報告もされています。

今回、この IE の脆弱性 （CVE-2010-0249）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 SP4 上の Internet Explorer 6 SP1
Windows XP SP2、SP3 の Internet Explorer 6、7、8
Windows XP Professional x64 Edition SP2 用の Internet Explorer 6、7、8
Windows Server 2003 SP2 の Internet Explorer 6、7、8
Windows Server 2003 SP2 for Itanium-based Systems の Internet Explorer 6、7、8
Windows Server 2003 x64 Edition SP2 用の Internet Explorer 6、7、8
Windows Vista SP なし、SP1、SP2 の Internet Explorer 7、8
Windows Vista x64 Edition SP なし、SP1、SP2 の Internet Explorer 7、8
Windows Server 2008 for 32-bit Systems SP なし、SP2 の Internet Explorer 7、8
Windows Server 2008 for Itanium-based Systems SP なし、SP2 の Internet Explorer 7
Windows Server 2008 for x64-based Systems SP なし、SP2 の Internet Explorer 7、8
Windows 7 for 32-bit Systems の Internet Explorer 8
Windows 7 for x64-based Systems の Internet Explorer 8
Windows Server 2008 R2 for x64-based Systems の Internet Explorer 8
Windows Server 2008 R2 for Itanium-based Systems の Internet Explorer 8

【対策案】

このレポート作成現在（2010 年 1 月 18 日）、修正プログラムはリリースされておりません。
修正プログラムのリリース、適用までは、脆弱性の影響を受けない代替ブラウザを使用することが推奨されます。

2010 年 1 月 22 日追記：
Microsoft 社から、修正プログラム（MS10-002）がリリースされています。
十分な検証の後、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（MS10-002）の適用を行うことが推奨されます。
http://www.microsoft.com/japan/technet/security/bulletin/ms10-002.mspx

修正プログラム（MS10-002）を適用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。

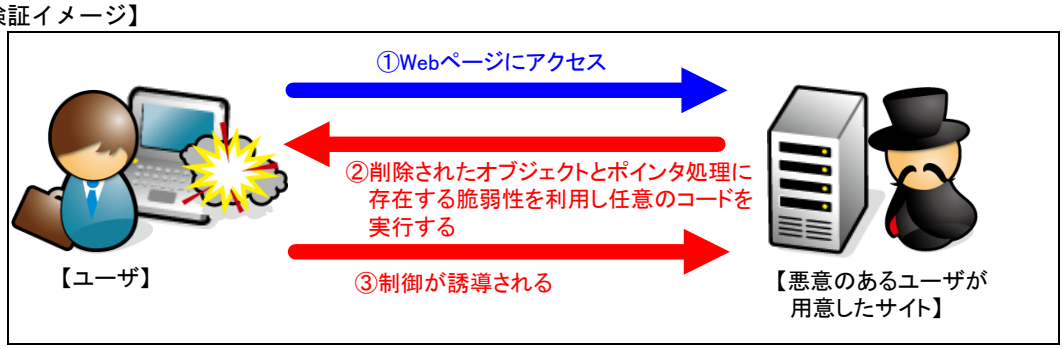
また、マイクロソフトセキュリティアドバイザリにて、以下の回避策が提示されています。

① インターネットおよびローカルイントラネットゾーンの設定を「高」に設定し、これらのゾーンで ActiveX コントロールおよびアクティブ スクリプトを実行する前にダイアログを表示する
② インターネットおよびイントラネット ゾーンで、アクティブスクリプトの実行前にダイアログを表示するように Internet Explorer を構成する、またはアクティブスクリプトを無効にするよう構成する
③ Internet Explorer 7 または Internet Explorer 6 Service Pack 2 で DEP（Data Execute Prevention：データ実行防止）を有効にする

【参考サイト】

マイクロソフト セキュリティ アドバイザリ(979352)
http://www.microsoft.com/japan/technet/security/advisory/979352.mspx
CVE-2010-0249
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0249

【検証イメージ】



【検証ターゲットシステム】

Windows XP SP2 IE6

【検証概要】

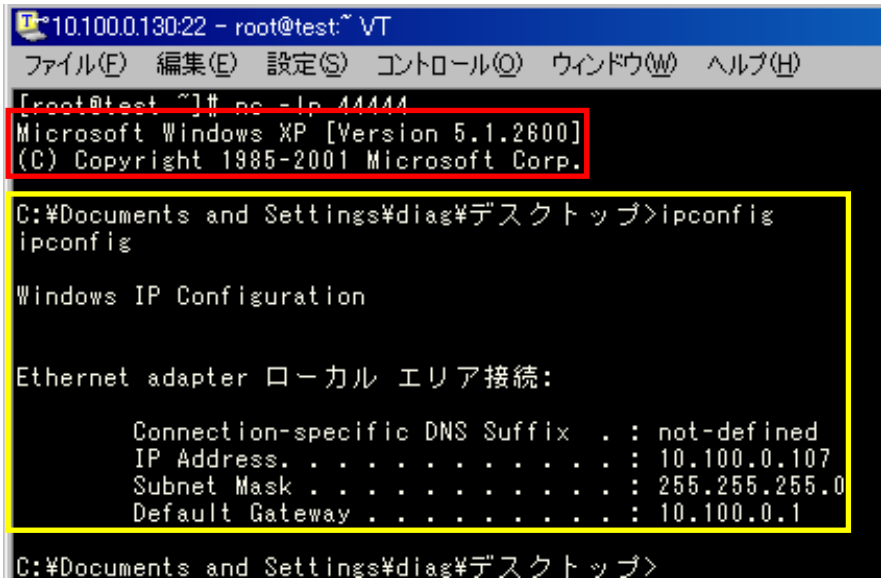
ターゲットシステムに、細工した Web コンテンツをロードさせることで任意のコードを実行させます。
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムを操作可能となります。
＊ 誘導先のシステムは CentOS 4 です。

NTTデータ・セキュリティ株式会社

【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（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。
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。

【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/