NTTデータ・セキュリティ株式会社

IE における解放済みメモリを使用する脆弱性(CVE-2010-0806)に関する検証レポート

2010/3/12

NTT データ・セキュリティ株式会社
辻 伸弘

【概要】

Microsoft 社の Internet Explorer (以下 IE) に解放済みメモリを使用する脆弱性 (CVE-2010-0806) 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。

今回、この IE の脆弱性 (CVE-2010-0806) 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
- Windows XP Service Pack 2 および 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、Windows Vista Service Pack 1 および Windows Vista Service Pack 2
- Windows Vista x64 Edition、Windows Vista x64 Edition Service Pack 1、Windows Vista x64 Edition 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
- Microsoft Windows 2000 Service Pack 4 上の Internet Explorer 6 Service Pack 1
- Windows XP Service Pack 2、Windows XP Service Pack 3 および Windows XP Professional x64 Edition Service Pack 2 用の Internet Explorer 6
- Windows Server 2003 Service Pack 2、Windows Server 2003 with SP2 for Itanium-based Systems および Windows Server 2003 x64 Edition Service Pack 2 用の Internet Explorer 6
- Windows XP Service Pack 2、Windows XP Service Pack 3 および Windows XP Professional x64 Edition Service Pack 2 用の Internet Explorer 7
- Windows Server 2003 Service Pack 2、Windows Server 2003 with SP2 for Itanium-based Systems および Windows Server 2003 x64 Edition Service Pack 2 用の Internet Explorer 7
- Windows Vista、Windows Vista Service Pack 1、Windows Vista Service Pack 2、Windows Vista x64 Edition、Windows Vista x64 Edition Service Pack 1 および Windows Vista x64 Edition Service Pack 2 の Internet Explorer 7
- Windows Server 2008 for 32-bit Systems および Windows Server 2008 for 32-bit Systems Service Pack 2 の Internet Explorer 7
- Windows Server 2008 for Itanium-based Systems および Windows Server 2008 for Itanium-based Systems Service Pack 2 の Internet Explorer 7
- Windows Server 2008 for x64-based Systems および Windows Server 2008 for x64-based Systems Service Pack 2 の Internet Explorer 7

【対策案】

このレポート作成現在（2010 年 3 月 12 日）、修正プログラムはリリースされておりません。
ただし、IE8 においてはこの脆弱性の影響を受けないとされているため IE8 への移行が推奨されます。
運用上、移行が困難である場合においては、修正プログラムのリリース、適用まで、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。

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。

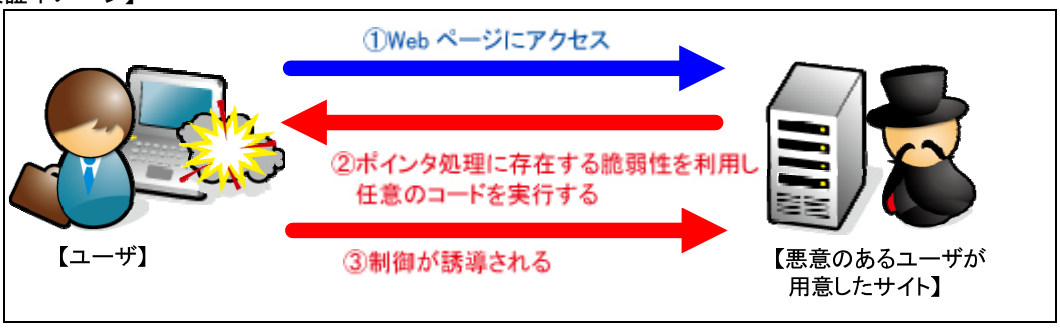
① iepeers.dll のピアファクトリクラスを無効にする。
② iepeers.dll のアクセス制御リスト（ACL）を変更する。
③ インターネットおよびローカル イントラネット セキュリティ ゾーンの設定を「高」に設定し、これらのゾーンで ActiveX コントロールおよびアクティブ スクリプトをブロックする。
④ インターネットおよびイントラネット ゾーンで、アクティブ スクリプトの実行前にダイアログを表示するように Internet Explorer を構成する、または アクティブ スクリプトを無効にするよう構成する。
⑤ Internet Explorer 6 Service Pack 2 または Internet Explorer 7 で DEP 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(981374)
http://www.microsoft.com/japan/technet/security/advisory/981374.mspx

CVE-2010-0806
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0806

【検証イメージ】



【検証ターゲットシステム】

Windows XP SP3 IE6 および 7

【検証概要】

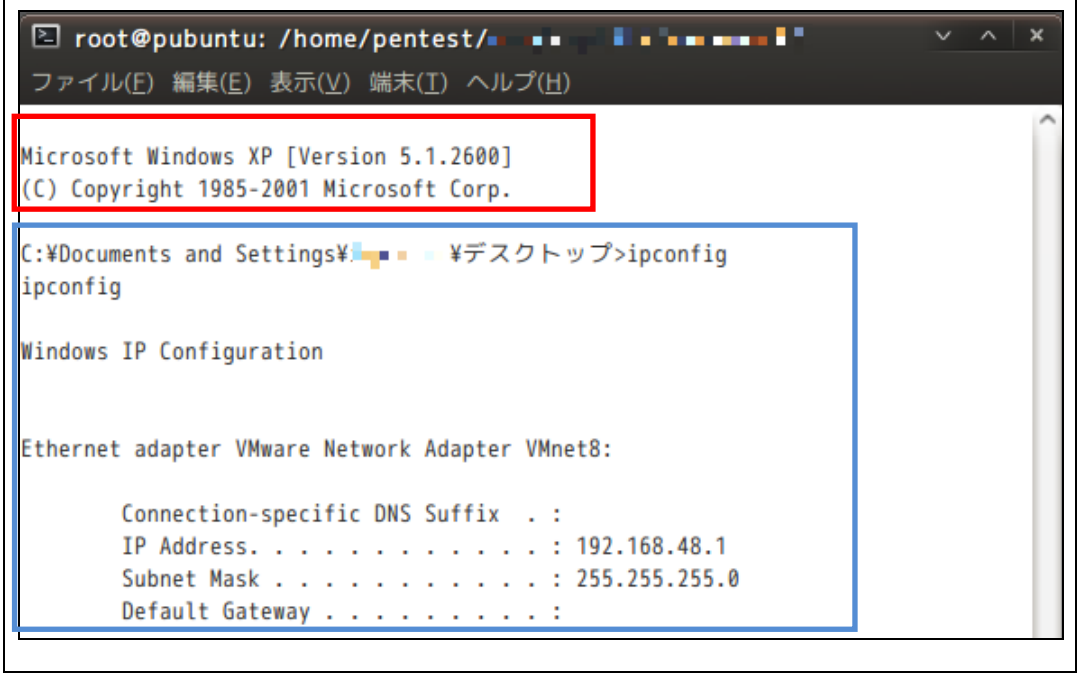
ターゲットシステムに、細工した Web コンテンツをロードさせることで任意のコードを実行させます。
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムを操作可能となります。
＊ 誘導先のシステムは Ubuntu 9.10 です。

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（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。
また、青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/