NTTデータ・セキュリティ株式会社

IE における VBScript と Windows Help ファイルの相互作用の方法に存在する脆弱性(CVE-2010-0483)に関する検証レポート

2010/3/3
2010/3/5(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 VBScript と Windows Help ファイルの相互作用の方法に脆弱性（CVE-2010-0483）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 ページの閲覧時にダイアログボックスを表示しユーザが「F1」キーを押すことで、ログオンしているユーザと同じ権限で任意のコードが実行される危険性があります。

今回、この IE における VBScript と Windows Help ファイルの相互作用の方法に存在する脆弱性（CVE-2010-0483）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
Windows XP SP2、SP3
Windows XP Professional x64 Edition SP2
Windows Server 2003 SP2
Windows Server 2003 with SP2 for Itanium-based Systems
Windows Server 2003 x64 Edition SP2

【対策案】

このレポート作成現在（2010 年 3 月 3 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。

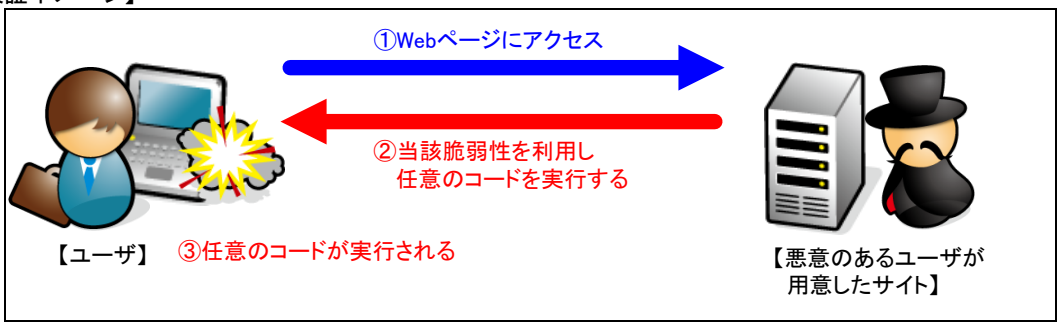
マイクロソフトセキュリティアドバイザリにて、以下の回避策が提示されています。

① Web サイトで表示された際に、「F1」 キーを押さない
② Windows ヘルプへのアクセスを制限する
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

【参考サイト】

マイクロソフト セキュリティ アドバイザリ (981169)
http://www.microsoft.com/japan/technet/security/advisory/981169.mspx
CVE-2010-0483
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0483

【検証イメージ】



【検証ターゲットシステム】
Windows XP SP3 IE7

【検証概要】
ターゲットシステムに、細工した Web コンテンツにアクセス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で電卓（calc.exe）を起動させるものです。

【検証結果】
下図が示すように、細工した Web コンテンツにアクセス後、ターゲットシステム上で電卓が起動しました。これにより、ターゲットシステム上で任意のコードが実行可能あると言えます。

ターゲットシステムの電卓の起動に成功した画面

NTTデータ・セキュリティ株式会社

2010 年 3 月 5 日追記：
以下に、電卓の起動以外の任意のコードを実行した追加検証を記載します。

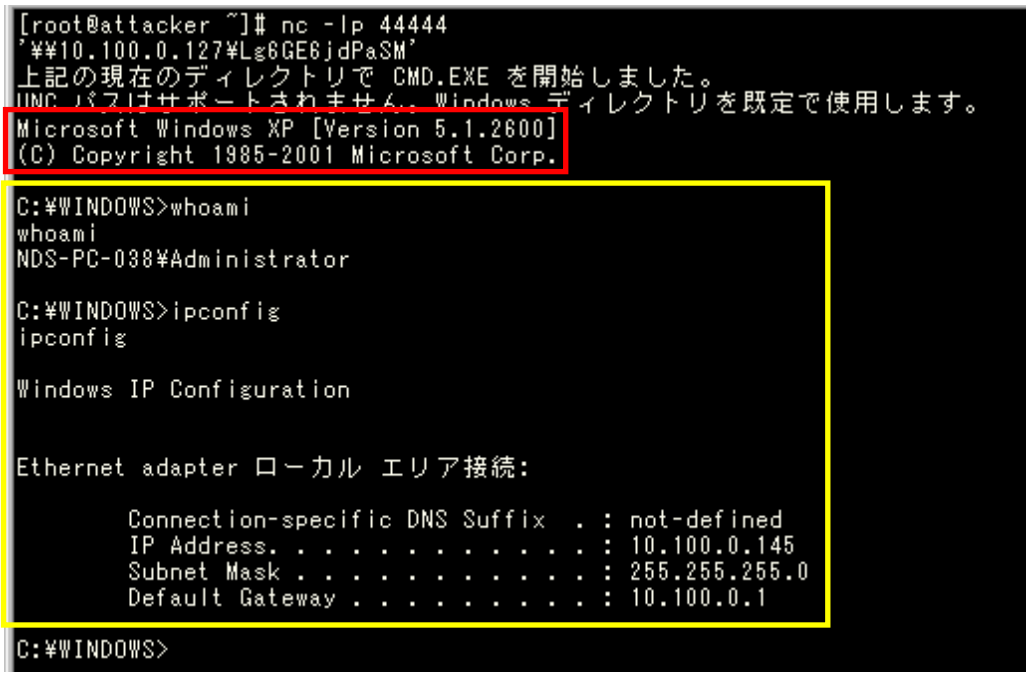
【追加検証概要】

ターゲットシステムに、細工した Web コンテンツにアクセスさせることで任意のコードを実行させます。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。

【追加検証結果】

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）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。
黄色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にログオンしているユーザと同じ権限で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/