NTTデータ・セキュリティ株式会社

IE の Style オブジェクト処理の脆弱性に関する検証レポート

2009/11/24
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 Style オブジェクト処理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 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 Style オブジェクト処理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】

IE6、または、IE7 がインストールされた Windows Vista、Server 2003、XP、2000 Server、98、98SE、ME、NT

【対策案】

このレポート作成現在（2009 年 11 月 24 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。
当該脆弱性は IE8 では影響を受けないため、IE8 へアップグレードすることも推奨されます。

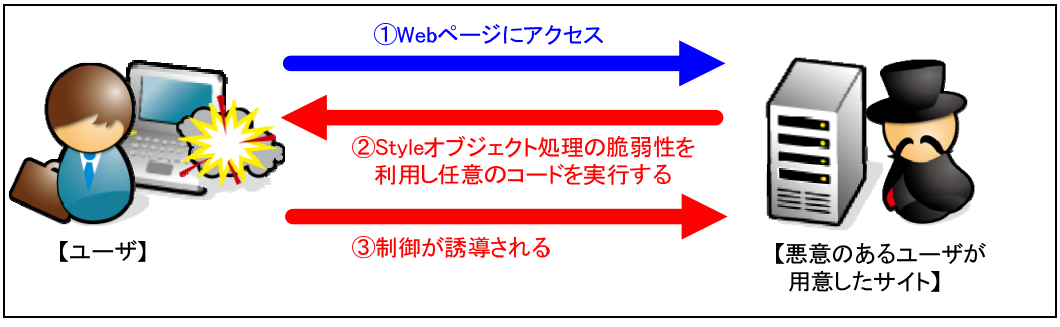
また、マイクロソフトセキュリティアドバイザリにて、以下の回避策が提示されています。

① 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(977981)
http://www.microsoft.com/japan/technet/security/advisory/977981.mspx

【検証イメージ】



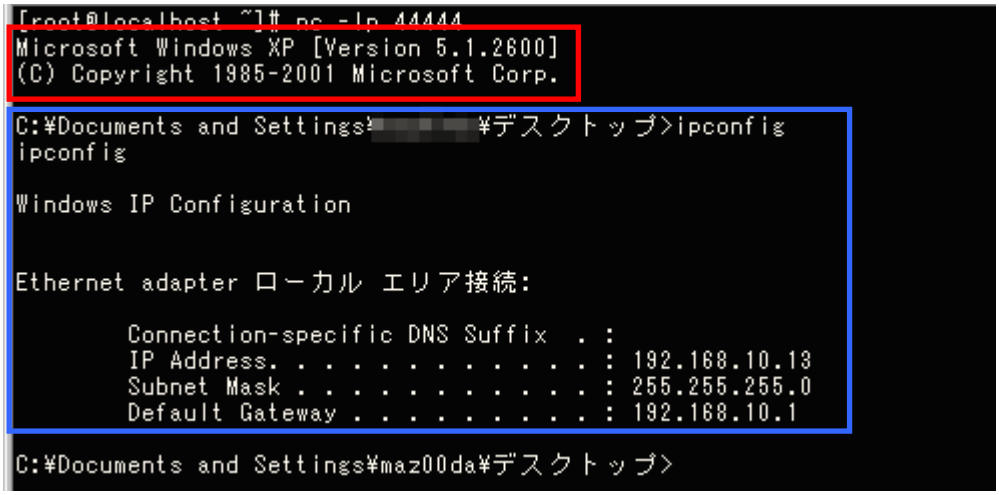
NTTデータ・セキュリティ株式会社

【検証ターゲットシステム】
Windows XP SP3 IE7
Windows Vista 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。*

【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。
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/