NTTデータ・セキュリティ株式会社

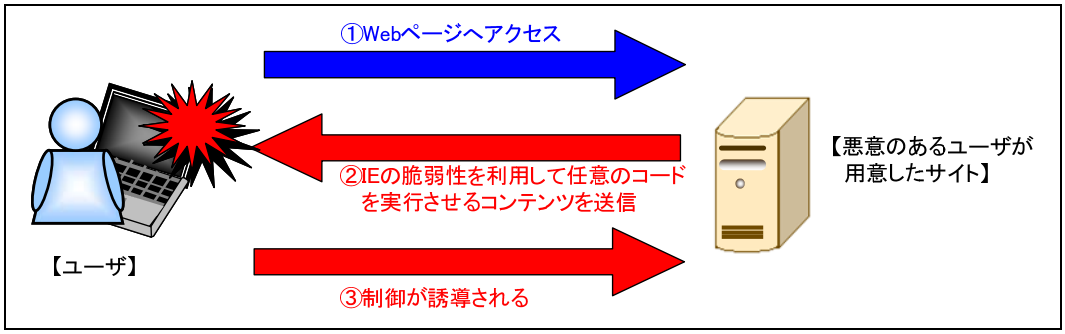
IE の削除されたオブジェクトへのアクセス処理の脆弱性(MS09-002)に関する検証レポート

2009/3/6
診断ビジネス部
辻　伸弘
松田　和之

【概要】

Internet Explorer(以下 IE)の削除されたオブジェクトへのアクセス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、そのローカルユーザと同じ権限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。(「被害イメージ」参照))

(被害イメージ)



今回、IE の削除されたオブジェクトへのアクセス処理の脆弱性 (MS09-002) 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】

以下のエディション上の Internet Explorer 7

- Windows XP SP2/SP3
- Windows XP Professional x64 Edition SP なし/SP2
- Windows Server 2003 SP1/SP2
- Windows Server 2003 x64 Edition SP なし/SP2
- Windows Server 2003 with SP1/SP2 for Itanium-based Systems
- Windows Vista SP なし/SP1
- Windows Vista x64 Edition SP なし/SP1
- Windows Server 2008 for 32-bit Systems
- Windows Server 2008 for x64-based Systems
- Windows Server 2008 for Itanium-based Systems

【対策案】

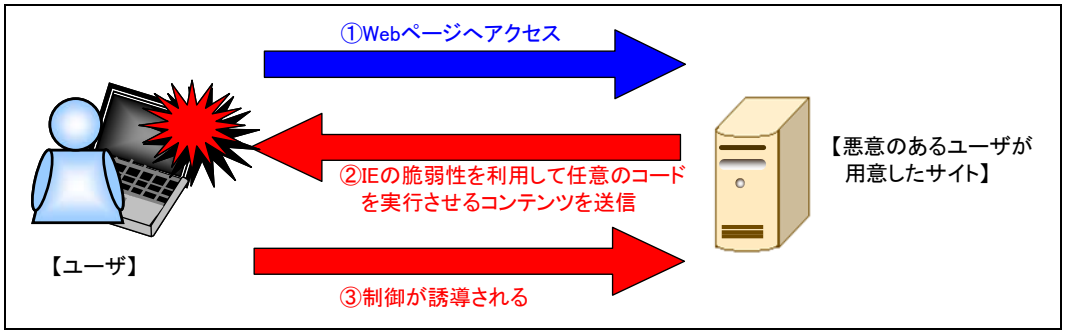
Microsoft 社から、修正プログラム (MS09-002) がリリースされています。
充分な検証の後、運用に支障をきたさないことをご確認の上、修正プログラム (MS09-002) の適用を行うことが推奨されます。

http://www.microsoft.com/japan/technet/security/bulletin/ms09-002.mspx

【参考サイト】

マイクロソフト セキュリティ情報 MS09-002 - 緊急
http://www.microsoft.com/japan/technet/security/bulletin/MS09-002.mspx

【検証イメージ】



【検証ターゲットシステム】

Microsoft Internet Explorer 7 がインストールされた Windows XP Service Pack 3
(Version: 7.0.5730.13)

【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 5 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。
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

```
[root@localhost pen-test]# nc -lp 4444
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:¥Documents and Settings¥Administrator¥デスクトップ>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter ローカル エリア接続:

        Connection-specific DNS Suffix  . : not-defined
        IP Address. . . . . . . . . . . . : 10.100.0.143
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.100.0.1

C:¥Documents and Settings¥Administrator¥デスクトップ>
```

NTTデータ・セキュリティ株式会社

【対策案】

Microsoft 社から、修正プログラム（MS09-002）がリリースされています。
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（MS09-002）の適用を行うことが推奨されます。

http://www.microsoft.com/japan/technet/security/bulletin/ms09-002.mspx

【参考サイト】

マイクロソフト セキュリティ情報 MS09-002 - 緊急

http://www.microsoft.com/japan/technet/security/bulletin/MS09-002.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/