NTT DATA
NTTデータ 先端技術株式会社

Microsoft Internet Explorer における mshtml CDwnBindInfo オブジェクトのメモリ利用不備により任意のコードが実行される脆弱性(CVE-2012-4792)に関する検証レポート

2013/01/09
2013/01/15 更新
NTT データ先端技術株式会社
辻　伸弘
泉田　幸宏
小田切　秀暁

【概要】

Microsoft Internet Explorer に、リモートより任意のコードが実行される脆弱性が発見されました。本脆弱性は、mshtml CDwnBindInfo オブジェクトが解放済みメモリを使用するために発生します。特別に細工された JavaScript を含むページを Internet Explorer が処理する際に、CDwnBindInfo オブジェクトを含む CDoc オブジェクトを作成します。これにより、このオブジェクトはポインタを削除せずに解放され、IE は不正なメモリアドレスを呼び出すよう強制されます。

本レポート作成（2013 年 1 月 9 日）時点において Microsoft 社から脆弱性への対策、回避策などのアナウンスが公開されております。しかし、本脆弱性を修正するバージョンはリリースされておらず、システムへの影響が大きいことから、脆弱性の再現性について検証を行いました。

2013 年 1 月 15 日追記：
Microsoft 社より、この脆弱性を修正するプログラム（MS13-008）がリリースされました。

【影響を受けるとされているシステム】

影響を受ける可能性が報告されているのは次の通りです。

- Windows XP Service Pack 3 上の Internet Explorer 6
- Windows XP Professional x64 Edition Service Pack 2 上の Internet Explorer 6
- Windows Server 2003 Service Pack 2 上の Internet Explorer 6
- Windows Server 2003 x64 Edition Service Pack 2 上の Internet Explorer 6
- Windows Server 2003 with SP2 for Itanium-based Systems 上の Internet Explorer 6
- Windows XP Service Pack 3 上の Internet Explorer 7
- Windows XP Professional x64 Edition Service Pack 2 上の Internet Explorer 7
- Windows Server 2003 Service Pack 2 上の Internet Explorer 7
- Windows Server 2003 x64 Edition Service Pack 2 上の Internet Explorer 7
- Windows Server 2003 with SP2 for Itanium-based Systems 上の Internet Explorer 7
- Windows Vista Service Pack 2 上の Internet Explorer 7
- Windows Vista x64 Edition Service Pack 2 上の Internet Explorer 7
- Windows Server 2008 for 32-bit Systems Service Pack 2 上の Internet Explorer 7
- Windows Server 2008 for x64-based Systems Service Pack 2 上の Internet Explorer 7
- Windows Server 2008 for Itanium-based Systems Service Pack 2 上の Internet Explorer 7
- Windows XP Service Pack 3 上の Internet Explorer 8
- Windows XP Professional x64 Edition Service Pack 2 上の Internet Explorer 8
- Windows Server 2003 Service Pack 2 上の Internet Explorer 8
- Windows Server 2003 x64 Edition Service Pack 2 上の Internet Explorer 8
- Windows Vista Service Pack 2 上の Internet Explorer 8
- Windows Vista x64 Edition Service Pack 2 上の Internet Explorer 8
- Windows Server 2008 for 32-bit Systems Service Pack 2 上の Internet Explorer 8
- Windows Server 2008 for x64-based Systems Service Pack 2 上の Internet Explorer 8
- Windows 7 for 32-bit Systems 上の Internet Explorer 8
- Windows 7 for 32-bit Systems Service Pack 1 上の Internet Explorer 8
- Windows 7 for x64-based Systems 上の Internet Explorer 8
- Windows 7 for x64-based Systems Service Pack 1 上の Internet Explorer 8
- Windows Server 2008 R2 for x64-based Systems 上の Internet Explorer 8
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 上の Internet Explorer 8
- Windows Server 2008 R2 for Itanium-based Systems 上の Internet Explorer 8
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 上の Internet Explorer 8

【対策案】

本レポート作成（2013 年 1 月 9 日）時点において、Microsoft 社から本脆弱性を修正するバージョンはリリースされておりません。修正プログラムがリリースされ適用するまでは、一時的に使用するブラウザを変更していただくことで影響を低減させることが可能です。

また、Microsoft 社からは Internet Explorer 9 および 10 では本脆弱性の影響は受けないとのアナウンスがあります。Windows Vista、Windows 7、Windows Server 2008 を使用している場合は、動作確認の上、Internet Explorer 9 にアップデートいただくことを推奨いたします。

アップデートが実行できない、または、Windows XP、Windows Server 2003 を使用している場合は、Microsoft 社から回避策として FixIT を適用する、EMET を使用する、Internet Explorer のセキュリティ設定を変更する方法が案内されています。以下の URL において具体的な回避策が記載されています。
・マイクロソフト セキュリティ アドバイザリ (2794220)
Internet Explorer の脆弱性により、リモートでコードが実行される
http://technet.microsoft.com/ja-jp/security/advisory/2794220

ただし、今回公開された脆弱性コードは FixIT を適用しても攻撃の成功を回避することはできませんでした。EMET を使用した場合、脆弱性コードを回避することを確認しました。

なお、Microsoft 社から本脆弱性を修正したバージョンがリリースされた際にはご利用環境への影響を確認の上、アップデートいただくことを推奨いたします。

2013 年 1 月 15 日追記：
Microsoft 社より、この脆弱性を修正するプログラム（MS13-008）がリリースされました。
当該脆弱性が修正された修正プログラムを適用していただくことを推奨いたします。

修正プログラムが適用された以下のシステムに対して、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。

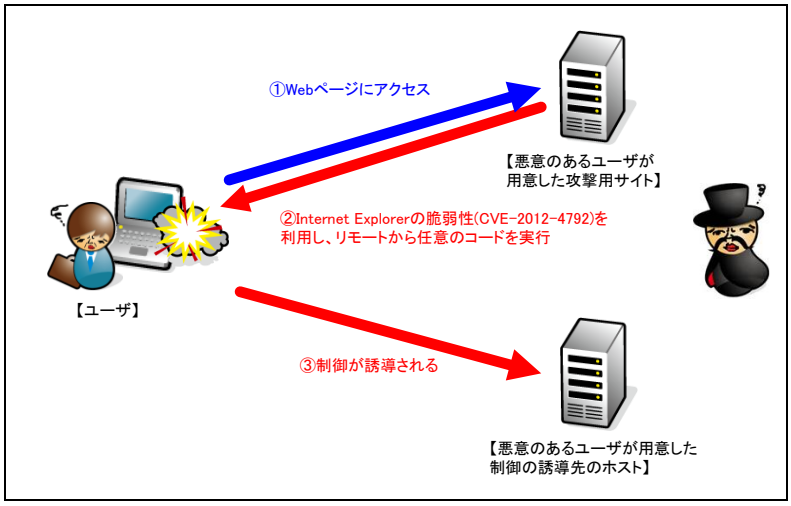
・Windows 7(日本語版)上の Internet Explorer 8(MS13-008 適用済み)
・Windows XP SP3（英語版）上の Internet Explorer 8(MS13-008 適用済み)

【参考サイト】
CVE-2012-4792
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4792

マイクロソフト セキュリティ アドバイザリ (2794220)
Internet Explorer の脆弱性により、リモートでコードが実行される
http://technet.microsoft.com/ja-jp/security/advisory/2794220

2013 年 1 月 15 日追記：
MS13-008: Internet Explorer のセキュリティ更新プログラム
http://support.microsoft.com/kb/2799329/ja

【検証イメージ】

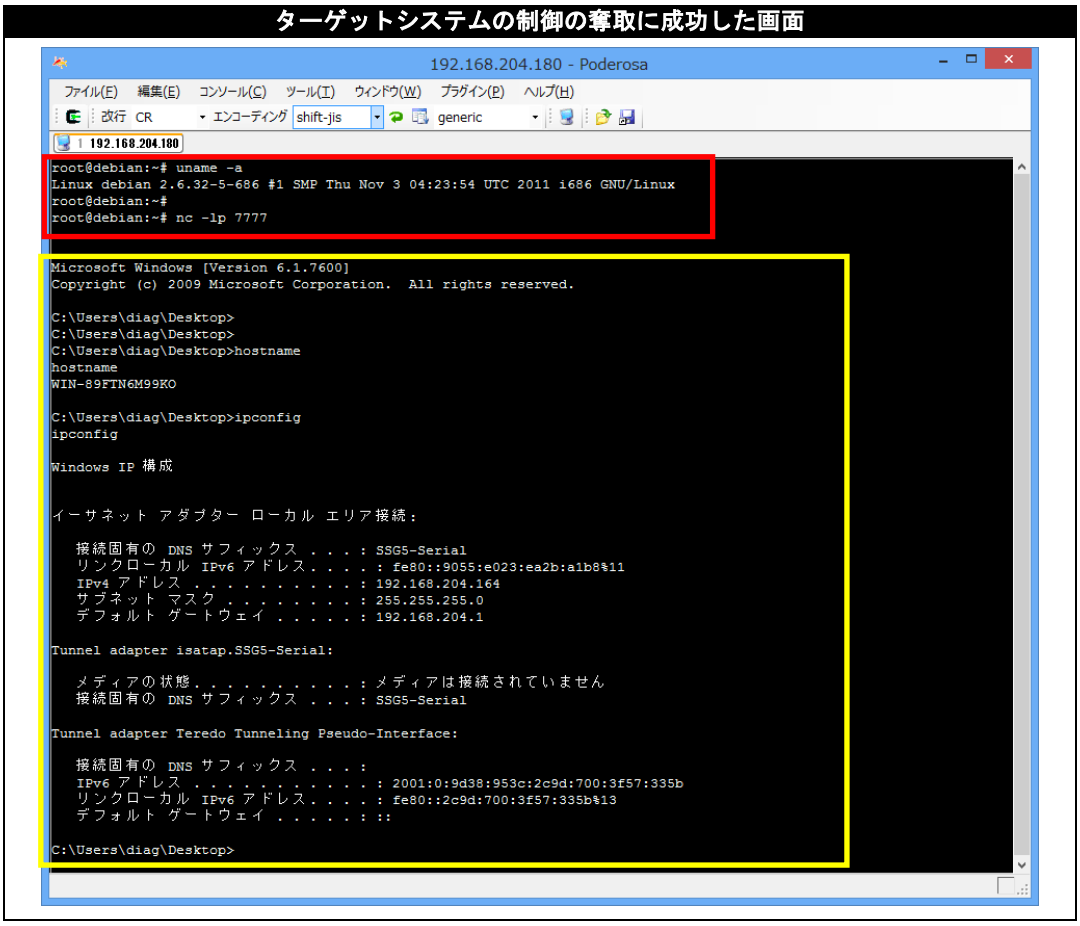


【検証ターゲットシステム】
Windows 7(日本語版)上の Internet Explorer 8
Windows XP SP3（英語版）上の Internet Explorer 8

【検証概要】
ターゲットシステム上の Internet Explorer で、細工した Web ページにアクセスさせることで、任意のコードを実行させます。ターゲットシステムは、悪意のあるユーザが用意したホストに制御が誘導されます。
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が操作可能となります。
＊誘導先のシステムは Debian です。

【検証結果】
下図の赤線で囲まれている部分に示すように、誘導先のコンピュータ（Debian）のコンソール上にターゲットシステム（windows 7）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に示すように、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 データ先端技術株式会社
セキュリティ事業部
TEL:03-5859-5422
http://security.intellilink.co.jp