NTTデータ 先端技術株式会社

Internet Explorer の mshtml.dll に存在する解放済みメモリを使用する脆弱性 (MS13-080)(CVE-2013-3893)に関する検証レポート

2013/10/2
2013/10/9 更新
NTT データ先端技術株式会社
辻 伸弘
泉田 幸宏

【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（CVE-2013-3893）が発見されました。この脆弱性を利用する攻撃コードは、Internet Explorer 8 が動作する Windows XP、または Internet Explorer8 および 9 が動作する Windows 7 を主な攻撃目標としています。
本脆弱性は mshtml.dll に存在しており、オブジェクトが解放される際に、オブジェクトへのポインタを削除しないために発生します。これにより、Internet Explorer は不正なメモリアドレスを呼び出すよう強制されます。

攻撃者は、細工された Web サイトを利用者に訪問させることにより、リモートから Internet Explorer を実行する利用者のユーザ権限で任意のコードを実行できる危険性があります。攻撃者は、細工された Web サイトにユーザを誘導することや、細工された Web サイトへのリンクを添付した電子メールを送信し、攻撃対象ユーザにファイルを開かせることで、ログオンしているユーザと同じ権限を奪取される危険性があります。

現時点（2013 年 10 月 2 日）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、脆弱性に対応した修正するプログラムはリリースされておりません。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。
2013/10/9 追記：
Microsoft 社より、この脆弱性を修正するプログラム（MS13-080）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】

- Windows XP Service Pack 3 上の Ineternet Explorer 6
- Windows XP Professional x64 Edition Service Pack 2 上の Ineternet Explorer 6
- Windows Server 2003 Service Pack 2 上の Ineternet Explorer 6
- Windows Server 2003 x64 Edition Service Pack 2 上の Ineternet Explorer 6
- Windows Server 2003 with SP2 for Itanium-based Systems 上の Ineternet Explorer 6

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

- Windows XP Service Pack 3 上の Ineternet Explorer 8
- Windows XP Professional x64 Edition Service Pack 2 上の Ineternet Explorer 8
- Windows Server 2003 Service Pack 2 上の Ineternet Explorer 8
- Windows Server 2003 x64 Edition Service Pack 2 上の Ineternet Explorer 8
- Windows Server 2003 with SP2 for Itanium-based Systems 上の Ineternet Explorer 8
- Windows Vista Service Pack 2 上の Ineternet Explorer 8

- Windows Vista x64 Edition Service Pack 2 上の Ineternet Explorer 8
- Windows Server 2008 for 32-bit Systems Service Pack 2 上の Ineternet Explorer 8
- Windows Server 2008 for x64-based Systems Service Pack 2 上の Ineternet Explorer 8
- Windows 7 for 32-bit Systems Service Pack 1 上の Ineternet Explorer 8
- Windows 7 for x64-based Systems Service Pack 1 上の Ineternet Explorer 8
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 上の Ineternet Explorer 8
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 上の Ineternet Explorer 8

- Windows Vista Service Pack 2 上の Ineternet Explorer 9
- Windows Vista x64 Edition Service Pack 2 上の Ineternet Explorer 9
- Windows Server 2008 for 32-bit Systems Service Pack 2 上の Ineternet Explorer 9
- Windows Server 2008 for x64-based Systems Service Pack 2 上の Ineternet Explorer 9
- Windows 7 for 32-bit Systems Service Pack 1 上の Ineternet Explorer 9
- Windows 7 for x64-based Systems Service Pack 1 上の Ineternet Explorer 9
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 上の Ineternet Explorer 9

- Windows 7 for 32-bit Systems Service Pack 1 上の Ineternet Explorer 10
- Windows 7 for x64-based Systems Service Pack 1 上の Ineternet Explorer 10
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 上の Ineternet Explorer 10
- Windows 8 for 32-bit Systems 上の Ineternet Explorer 10
- Windows 8 for 64-bit Systems 上の Ineternet Explorer 10
- Windows Server 2012 上の Ineternet Explorer 10
- Windows RT 上の Ineternet Explorer 10

- Windows 8.1 for 32-bit Systems 上の Ineternet Explorer 11
- Windows 8.1 for 64-bit Systems 上の Ineternet Explorer 11
- Windows Server 2012 R2 上の Ineternet Explorer 11
- Windows RT 8.1 上の Ineternet Explorer 11

【対策案】

本レポートの作成時点（2013 年 10 月 2 日）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 社では、回避策として「Fix it」を適用する、「EMET」を導入する、Internet Explorer のセキュリティゾーン設定を「高」へ変更する方法がアナウンスされております。以下の URL において具体的な回避策が記載されております。

マイクロソフト セキュリティ アドバイザリ (2887505)
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/2887505

2013/10/9 追記：
Microsoft 社より、この脆弱性を修正するプログラム（MS13-080）がリリースされました。
動作確認の上、本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 SP1 上の Internet Explorer 9(MS13-080 適用済み)、および Office 2007

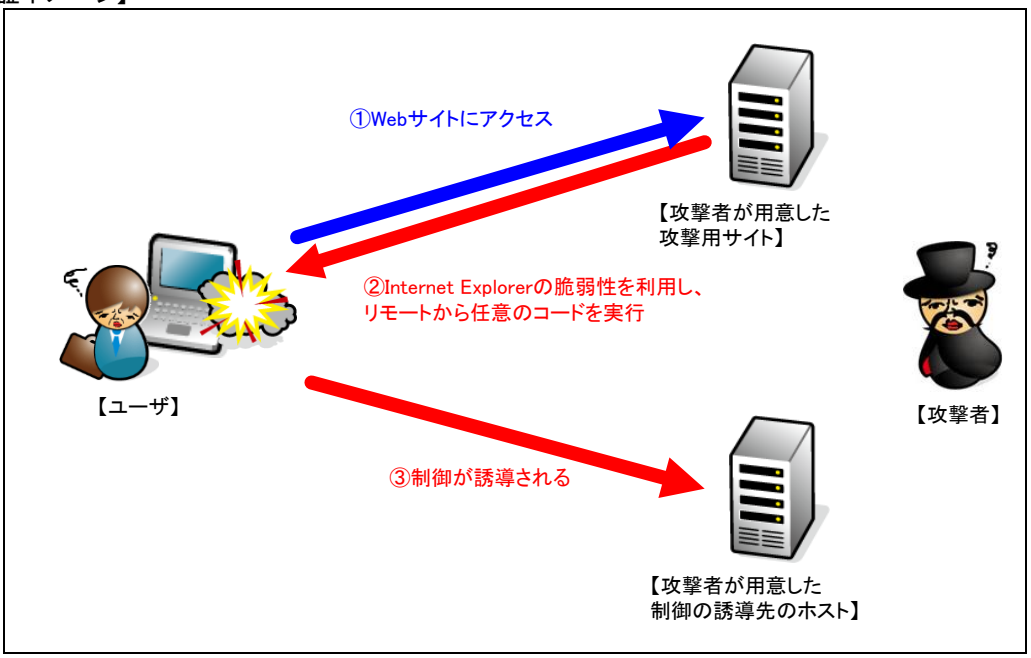
【参考サイト】
CVE-2013-3893
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3893

マイクロソフト セキュリティ アドバイザリ (2887505)
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/2887505

Internet Explorer の脆弱性対策について(CVE-2013-3893)
http://www.ipa.go.jp/security/ciadr/vul/20130918-ms.html

2013/10/9 追記：
MS13-080: Internet Explorer 用の累積的なセキュリティ更新プログラム (2879017)
https://technet.microsoft.com/ja-jp/security/bulletin/ms13-080

【検証イメージ】



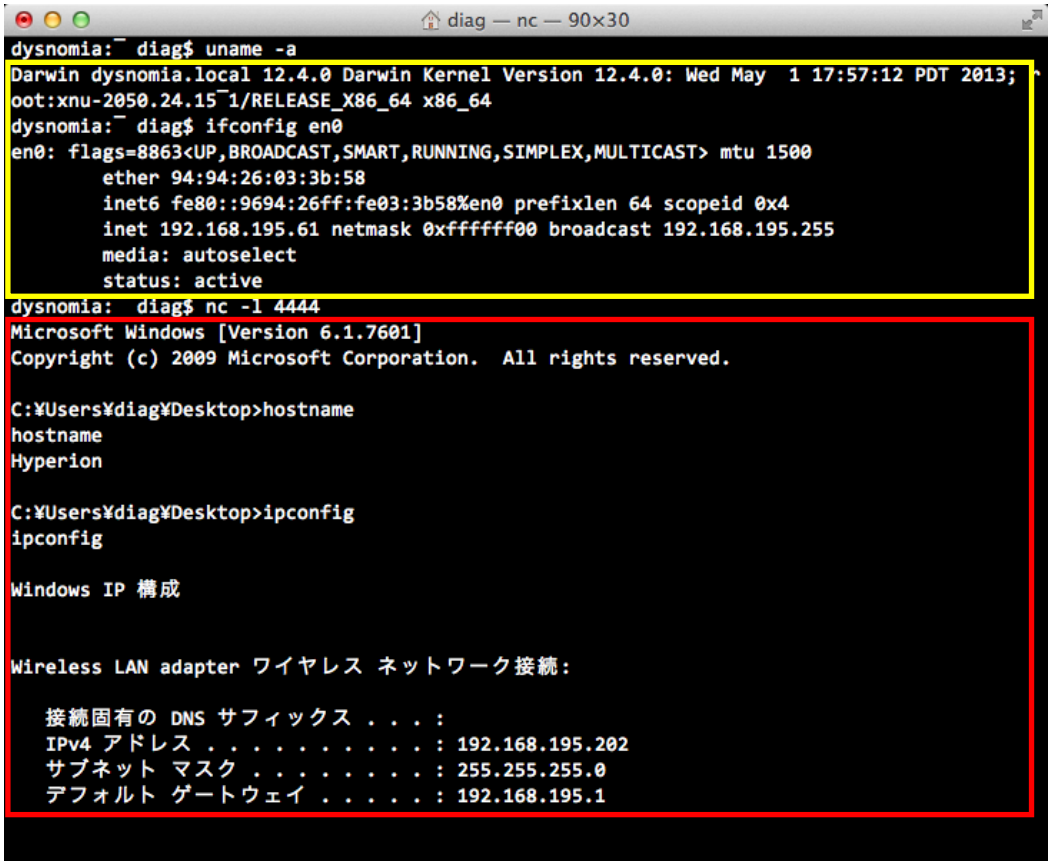
【検証ターゲットシステム】
Windows 7 SP1 上の Internet Explorer 9、および Office 2007

【検証概要】
ターゲットシステム上の Internet Explorer で、細工した Web サイト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 Mac OSX です。*

【検証結果】
下図は、攻撃後の誘導先のシステム画面です。

下図は、誘導先のコンピュータ（Mac OSX）の画面です。黄線で囲まれている部分は、誘導先のコンピュータのホスト情報です。一方で、赤線で囲まれている部分は、ターゲットシステム（Windows 7）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://intellilink.co.jp