NTT DATA
NTTデータ 先端技術株式会社

Microsoft Internet Explorer 8 における mshtml CGenericElement 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-2013-1347)に関する検証レポート

2013/05/07
2013/5/15 更新
NTT データ先端技術株式会社
辻　伸弘
小田切　秀暁
渡邊　尚道

【概要】

Microsoft Internet Explorer 8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 CGenericElement 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 Web ページを Internet Explorer が処理する際に、CGenericElement オブジェクトを含む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 5 月 7 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、本脆弱性に対応した修正プログラム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。
2013/5/15 追記：
Microsoft 社より、この脆弱性を修正するプログラム（MS13-038）がリリースされました。
2013/5/10 追記：
Microsoft 社より、本脆弱性の暫定対処プログラム「Microsoft Fix it 50992」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 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 Service Pack 1 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 Service Pack 1 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 5 月 7 日）時点において、Microsoft 社から本脆弱性に対応した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 8 以外のバージョン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 以降にアップデートいただくことを推奨いたします。

アップデートができない場合は、Microsoft 社から回避策として 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。
なお、Windows XP、Windows Server 2003 は Internet Explorer9 以降にアップデートすることができません。
2013/5/15 追記：
Microsoft 社より、この脆弱性を修正するプログラム（MS13-038）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(日本語版)上の Internet Explorer 8(MS13-038 適用済み)

2013/5/10 追記：
Microsoft 社より、本脆弱性の暫定対処プログラム「Microsoft Fix it 50992」がリリースされました。

・マイクロソフト セキュリティ アドバイザリ (2847140)
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/2847140

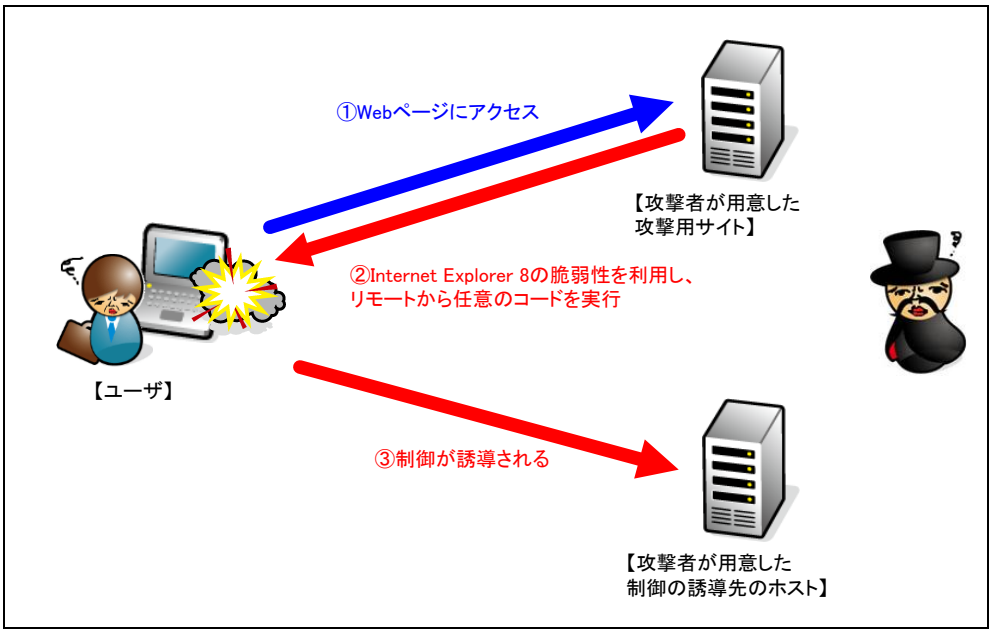
【参考サイト】
CVE-2013-1347
http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2013-1347

マイクロソフト セキュリティ アドバイザリ (2847140)
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/2847140

2013/5/15 追記：
MS13-038: Internet Explorer のセキュリティ更新プログラム
https://technet.microsoft.com/ja-jp/security/bulletin/ms13-038

2013/5/10 追記：
Microsoft Security Advisory: Vulnerability in Internet Explorer 8 could allow remote code execution
http://support.microsoft.com/kb/2847140

【検証イメージ】



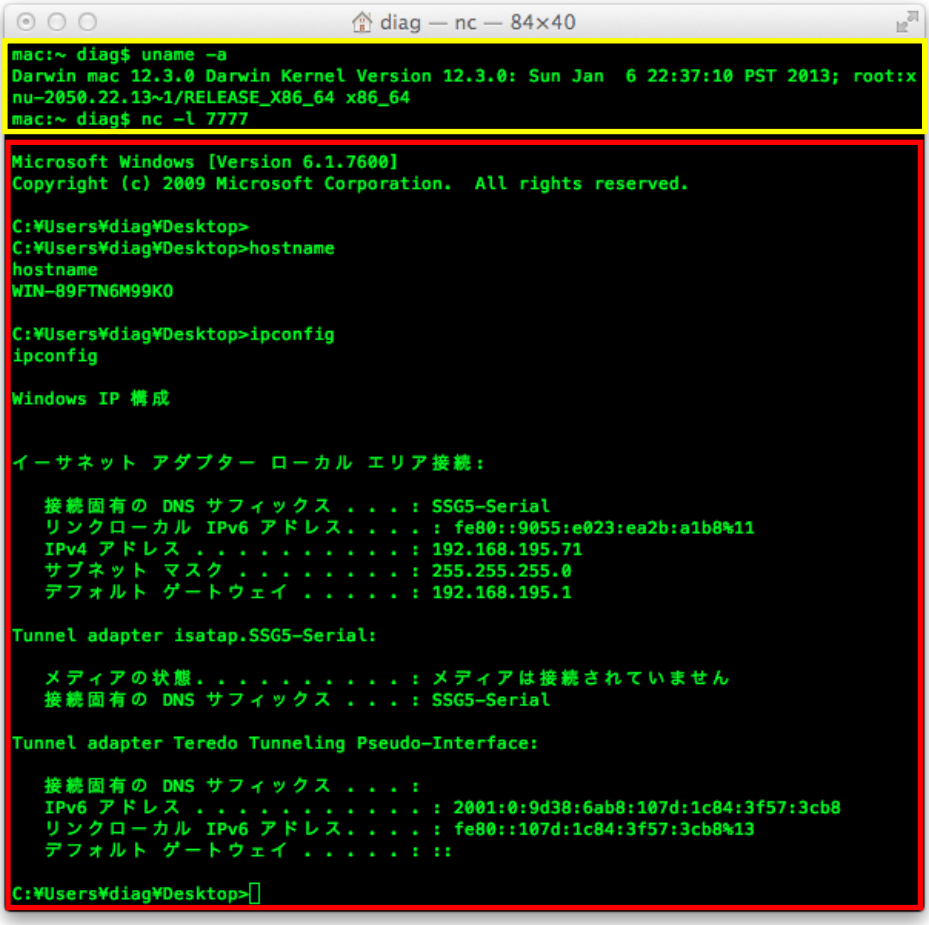
【検証ターゲットシステム】
Windows 7 上の Internet Explorer 8

【検証概要】
ターゲットシステム上で、攻撃者が作成した Web ページを閲覧させることで、攻撃コードを実行させます。それによって、ターゲットシステムにおいて任意のコードを実行させます。
ターゲットシステムは、攻撃者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 MacOS X 10.8.3 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（MacOS X）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、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