NTTデータ 先端技術株式会社

Microsoft Internet Explorer における CMshtmlEd::Exec 関数処理の不備により任意のコードが実行される脆弱性に関する検証レポート

2012/9/18
2012/9/24 更新
NTT データ先端技術株式会社
辻 伸弘
渡邊 尚道
小松 徹也

【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、Internet Explorer の CMshtmlEd::Exec 関数処理における解放済みメモリの使用により任意のコードを実行させることが可能です。

本レポート作成（2012 年 9 月 18 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が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。

2012 年 9 月 24 日追記：
Microsoft 社より、この脆弱性を修正するプログラム（MS12-063）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 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
- Windows Vista Service Pack 2 上の Internet Explorer 9
- Windows Vista x64 Edition Service Pack 2 上の Internet Explorer 9
- Windows Server 2008 for 32-bit Systems Service Pack 2 上の Internet Explorer 9
- Windows Server 2008 for x64-based Systems Service Pack 2 上の Internet Explorer 9
- Windows 7 for 32-bit Systems 上の Internet Explorer 9
- Windows 7 for 32-bit Systems Service Pack 1 上の Internet Explorer 9
- Windows 7 for x64-based Systems 上の Internet Explorer 9
- Windows 7 for x64-based Systems Service Pack 1 上の Internet Explorer 9
- Windows Server 2008 R2 for x64-based Systems 上の Internet Explorer 9
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 上の Internet Explorer 9

（2012 年 9 月 18 日時点）

【対策案】

本レポート作成（2012 年 9 月 18 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を推奨いたします。

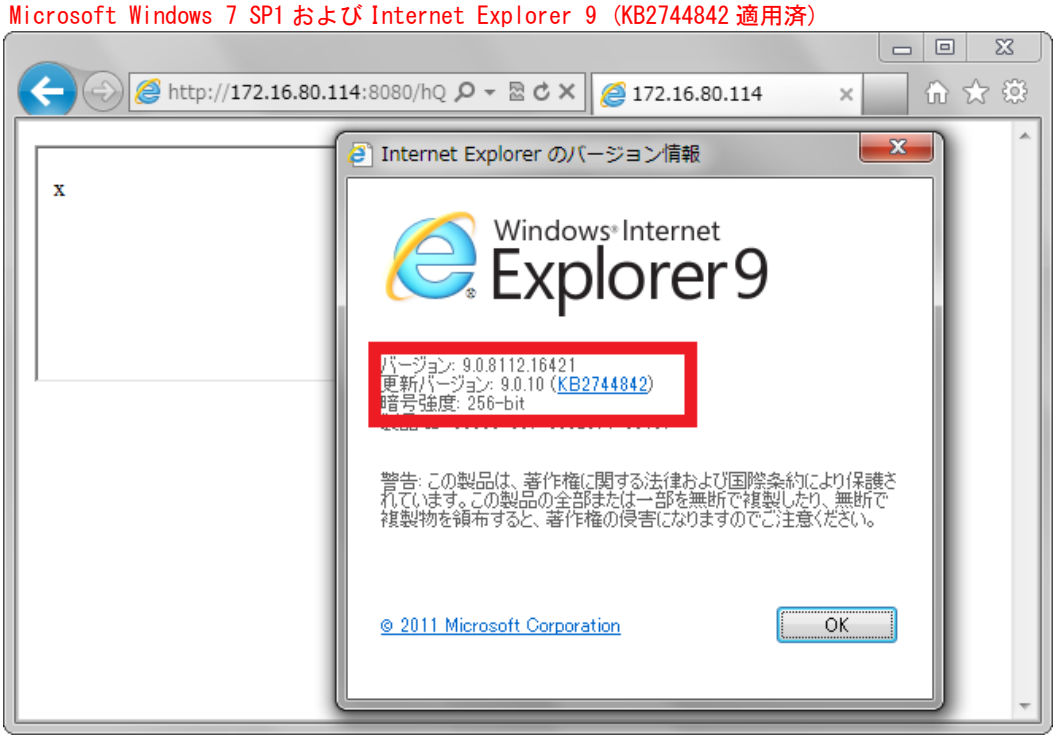
なお、Microsoft 社から本脆弱性を修正したバージョンがリリースされた際にはご利用環境への影響を確認の上、アップデートいただくことを推奨いたします。

Microsoft Windows Update サイト
http://windowsupdate.microsoft.com/

2012 年 9 月 24 日追記：
Microsoft 社より、この脆弱性を修正するプログラム（MS12-063）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。

・Microsoft Windows 7 SP1 および Internet Explorer 9（KB2744842 適用済）



【参考サイト】

マイクロソフト セキュリティ アドバイザリ (2757760)
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/2757760

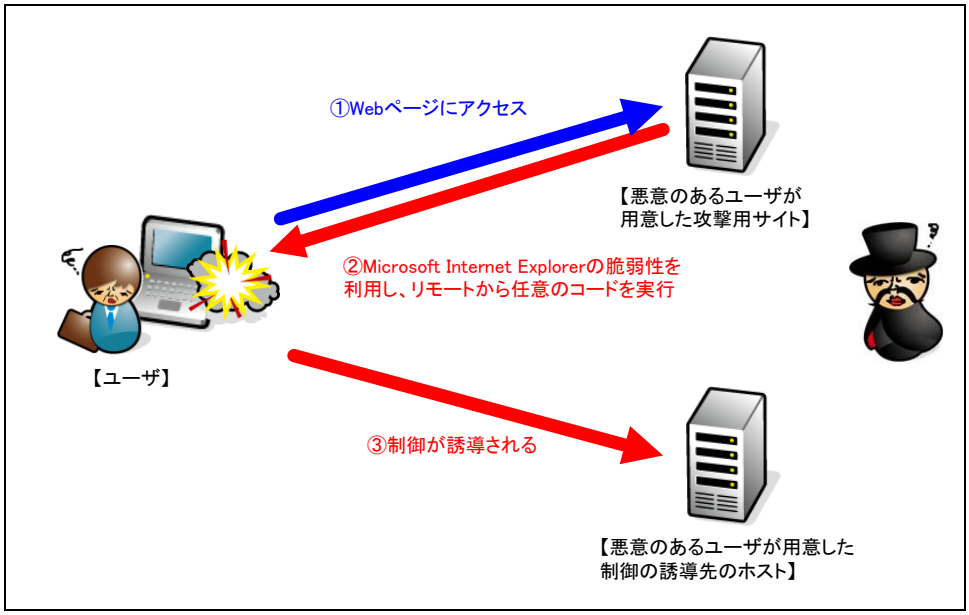
Microsoft IE CMshtmlEd::Exec() Function Use-after-free Remote Code Execution
http://www.osvdb.org/show/osvdb/85532

VU#480095: Microsoft Internet Explorer 7/8/9 contain a use-after-free vulnerability
http://www.kb.cert.org/vuls/id/480095

Secunia Advisory SA50626: Microsoft Internet Explorer Unspecified Code Execution Vulnerability
http://secunia.com/advisories/50626/

2012 年 9 月 24 日追記：
マイクロソフト セキュリティ情報 MS12-063 - 緊急
Internet Explorer 用の累積的なセキュリティ更新プログラム (2744842)
http://technet.microsoft.com/ja-jp/security/bulletin/ms12-063

【検証イメージ】



【検証ターゲットシステム】
・Microsoft Windows 7 SP1 および Internet Explorer 8
・Microsoft Windows 7 SP1 および Internet Explorer 9

【検証概要】
ターゲットシステム上で、悪意のあるユーザが作成した 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、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。

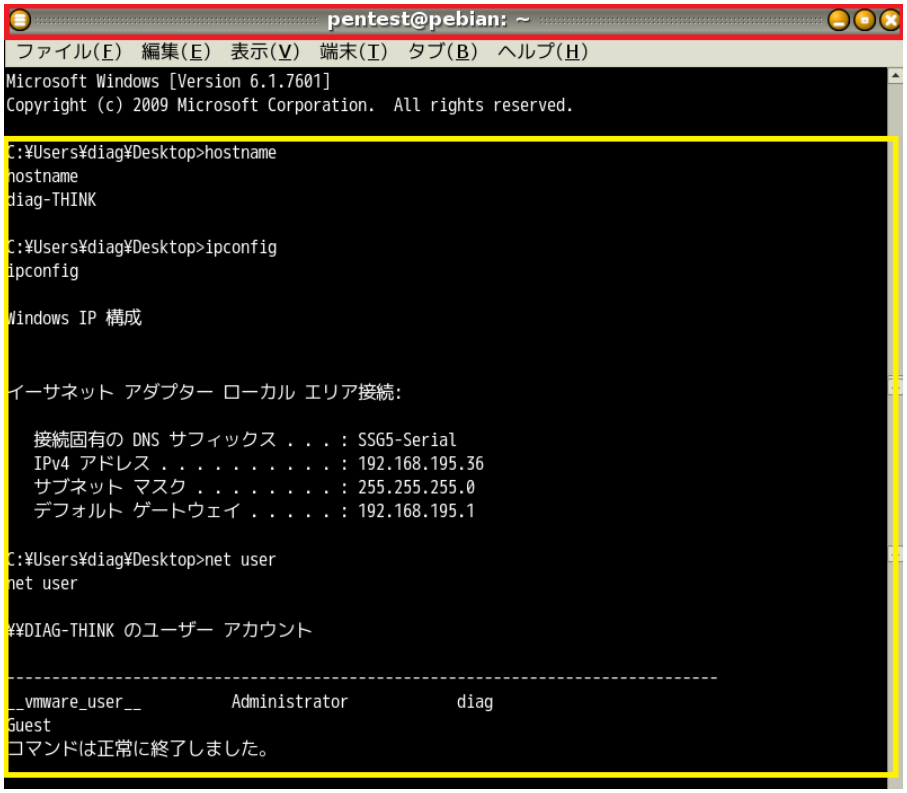
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムが操作可能となります。
＊ 誘導先のシステムは Debian です。

【検証結果】

下図は、攻撃後の誘導先のシステム画面です。

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（Debian）のターミナ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　営業担当　サービス企画戦略グループ
TEL：03-5859-5422
http://security.intellilink.co.jp