NTTデータ・セキュリティ株式会社

IE(mshtml.dll)の CSS 解析処理におけるメモリ破壊の脆弱性(CVE-2010-3971)に関する検証レポート

2011/01/12
NTT データ・セキュリティ株式会社
辻 伸弘
小田切 秀暁

【概要】

Microsoft 社の Internet Explorer（以下 IE）に、リモートから攻撃可能なメモリ破壊の脆弱性（CVE-2010-3971）が発見されました。

この脆弱性は mshtml.dll に存在します。CSS の解析処理実行時に、CStyleSheet オブジェクトに格納されている配列を処理する際、メモリ上のヒープポインタが適切に初期化されない可能性があります。

この脆弱性により、細工された Web ページの閲覧、Outlook や OutlookExpress による細工された HTML メールプレビューなどで、ローカルユーザと同じ権限が奪取される危険性があります。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。

今回、この IE の脆弱性（CVE-2010-3971）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およびアプリケーション】

影響を受ける可能性が報告されているシステムおよびアプリケーションは次の通りです。

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

【対策案】

このレポート作成現在（2011 年 1 月 12 日）修正プログラムはリリースされていません。
マイクロソフト社は以下の回避策が提示しています。

① Enhanced Mitigation Experience Toolkit (EMET) を使用する
② インターネットおよびローカル イントラネット セキュリティ ゾーンの設定を「高」に設定し、これらのゾーンで ActiveX コントロールおよびアクティブ スクリプトをブロックする

詳細および回避策の影響については、
「マイクロソフトセキュリティアドバイザリ(2488013)」の「回避策」を参照ください。
http://www.microsoft.com/japan/technet/security/advisory/2488013.mspx

【参考サイト】

マイクロソフト社のセキュリティ アドバイザリ (2488013)
http://www.microsoft.com/japan/technet/security/advisory/2488013.mspx
CVE-2010-3971
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3971

【検証イメージ】

【検証ターゲットシステム】

Windows 7 および Internet Explorer 8 (2011 年 1 月 12 日時点にリリースされているすべての修正プログラムを適用済み)

NTTデータ・セキュリティ株式会社

【検証概要】

ターゲットシステムに IE を通じて、細工された Web ページを閲覧させ、IE の脆弱性を利用した攻撃コードを実行することで任意のコードを実行させます。

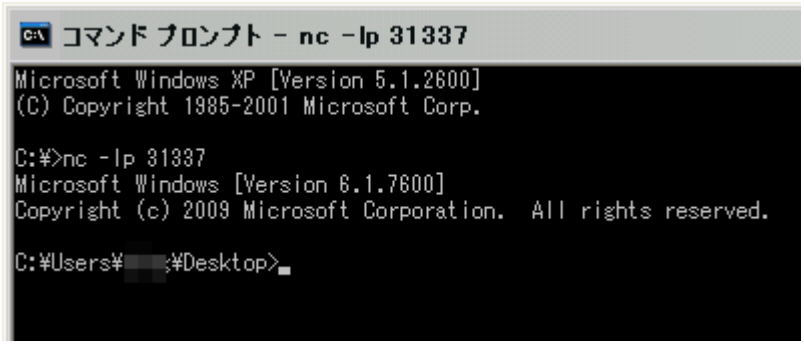
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるように誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムの操作が可能となります。
＊ 誘導先のシステムは Windows XP です。

【検証結果】

下図が示すように、誘導先のコンピュータ（Windows XP）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。

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・セキュリティ株式会社
企画部　広報グループ
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/