NTTデータ・セキュリティ株式会社

IE の DOM 処理においてリモートから攻撃可能なメモリ破壊の脆弱性 (CVE-2011-1256,MS11-050)に関する検証レポート

2011/06/20
NTT データ・セキュリティ株式会社
辻　伸弘
小田切　秀暁
泉田　幸宏

【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-2011-1256)が発見されました。

この脆弱性は IE の DOM 変更処理に存在します。IE が正しく初期化されていないオブジェクトや削除されたオブジェクトを処理する際に、メモリ破壊を引き起こす可能性があります。

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-2011-1256)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アプリケーション】

現在のところ、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 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 および Windows 7 for 32-bit Systems Service Pack 1 Internet Explorer 8
- Windows 7 for x64-based Systems および Windows 7 for x64-based Systems Service Pack 1 Internet Explorer 8
- Windows Server 2008 R2 for x64-based Systems および Windows Server 2008 R2 for x64-based Systems Service Pack 1 Internet Explorer 8
- Windows Server 2008 R2 for Itanium-based Systems および Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Explorer 8

【対策案】
Microsoft 社より、この脆弱性を修正するプログラム(MS11-050)がリリースされております。
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。

また、Microsoft 社では以下の回避策を提示しております。修正プログラムの適用が困難である場合はご検討下さい。

回避策:
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。
③ 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 ゾーンで、アクティブ スクリプトが実行される前にダイアログを表示するように設定する。
④ 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 ゾーンで、アクティブ スクリプトの実行を無効化する。

【参考サイト】
マイクロソフト セキュリティ情報 MS11-050
Internet Explorer 用の累積的なセキュリティ更新プログラム(2530548)
http://www.microsoft.com/japan/technet/security/bulletin/ms11-050.mspx

CVE-2011-1256
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1256

【検証イメージ】

【検証ターゲットシステム】
Windows XP Professional SP3 および Internet Explorer 7(XP は SP3 適用直後の状態)

【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 Linux です。

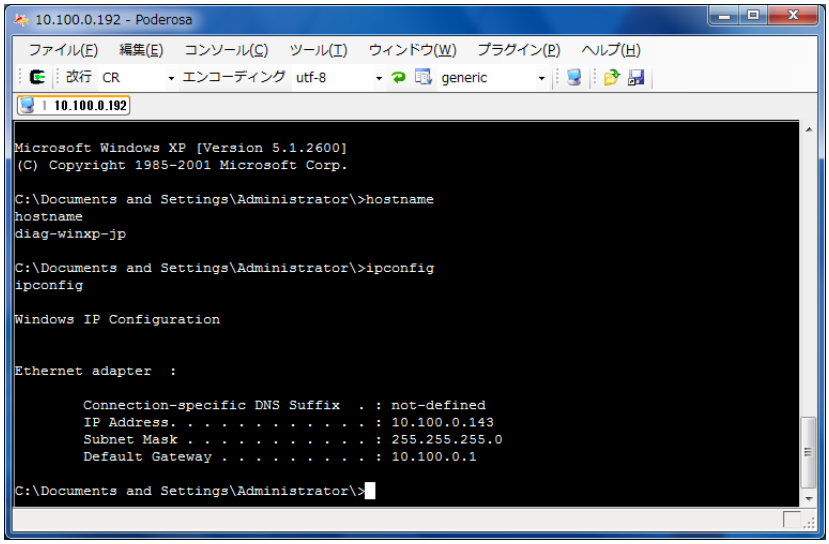
NTTデータ・セキュリティ株式会社

【検証結果】

下図が示すように、誘導先のコンピュータ(Debian)上にターゲットシステム(Windows XP) 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
営業本部　戦略営業グループ
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/