NTT DATA
NTTデータ 先端技術株式会社

Microsoft XML Core Services(MSXML)におけるメモリ破壊により、任意のコードが実行される脆弱性(CVE-2012-1889)に関する検証レポート

2012/6/20
NTT データ先端技術株式会社
辻 伸弘
小田切 秀暁

【概要】

Windows に使用されている XML Core Services に、メモリ破壊の脆弱性（CVE-2012-1889）が存在します。この脆弱性は、Microsoft XML Core Services(MSXML)が初期化されていないメモリ内のオブジェクトにアクセスを試みる場合に発生します。

この脆弱性を悪用して、攻撃者はターゲットホスト上で任意のコードの実行が可能です。攻撃者は、Internet Explorer 経由で MSXML を呼び出すように特別に細工された Web サイトにユーザを誘導する等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。

今回、Microsoft XML Core Services の脆弱性（CVE-2012-1889）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・アプリケーション】

- Windows XP Service Pack 3 Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows XP Professional x64 Edition Service Pack 2 Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows Server 2003 Service Pack 2 Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows Server 2003 x64 Edition Service Pack 2 Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows Server 2003 with SP2 for Itanium-based Systems Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows Vista Service Pack 2 Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows Vista x64 Edition Service Pack 2 Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows Server 2008 for 32-bit Systems Service Pack 2 (*) Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows Server 2008 for x64-based Systems Service Pack 2 (*) Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows Server 2008 for Itanium-based Systems Service Pack 2 Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows 7 for 32-bit Systems Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows 7 for 32-bit Systems Service Pack 1 Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows 7 for x64-based Systems Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows 7 for x64-based Systems Service Pack 1 Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows Server 2008 R2 for x64-based Systems (*) Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (*) Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows Server 2008 R2 for Itanium-based Systems Microsoft XML コア サービス 3.0, 4.0, 6.0
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Microsoft XML コア サービス 3.0, 4.0, 6.0
- Microsoft Office 2003 Service Pack 3 Microsoft XML コア サービス 5.0
- Microsoft Office 2007 Service Pack 2 Microsoft XML コア サービス 5.0
- Microsoft Office 2007 Service Pack 3 Microsoft XML コア サービス 5.0

(*) Server Core インストールは影響を受けます。

【対策案】

このレポート作成現在（2012 年 6 月 20 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セキュリティアドバイザリで回避策を提示しています。

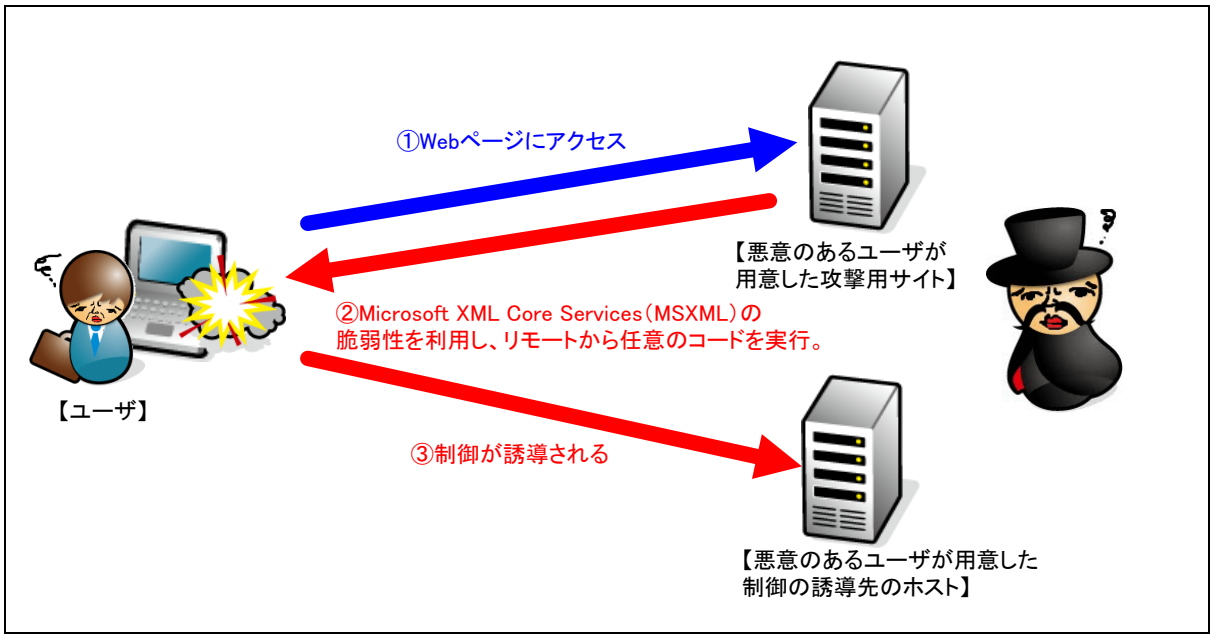
マイクロソフト セキュリティ アドバイザリ (2719615)
XML コアサービスの脆弱性により、リモートでコードが実行される
http://technet.microsoft.com/ja-jp/security/advisory/2719615

① この脆弱性の攻撃方法をブロックするマイクロソフト Fix It ソリューションを適用する
② Enhanced Mitigation Experience Toolkit(EMET) を使用する
③ Internet Explorer をインターネットおよびイントラネット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構成する、または アクティブ スクリプトを無効にするよう構成する

【参考サイト】
CVE-2012-1889
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1889

Microsoft Windows 等の脆弱性の回避策について(KB2719615)(CVE-2012-1889)
http://www.ipa.go.jp/security/ciadr/vul/20120618-windows.html

【検証イメージ】



【検証ターゲットシステム】
Windows XP SP3 Internet Explorer 7

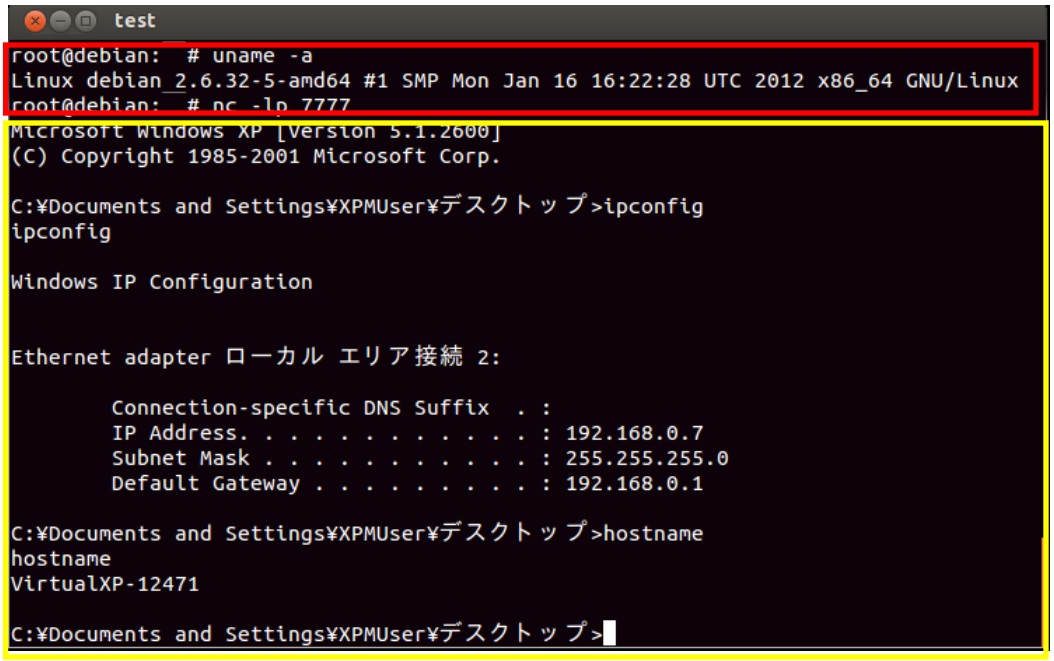
【検証概要】
ターゲットシステムに、悪意のあるユーザが用意した Web ページを閲覧させることで、攻撃コードを実行させます。それによって、ターゲットシステムにおいて任意のコードを実行させます。
ターゲットシステムは、悪意のあるユーザが用意したホストに制御が誘導されます。

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 6.0 です。

【検証結果】

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）のコンソール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。
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/