NTTデータ 先端技術株式会社

Windows コモンコントロールの脆弱性により、任意のコードが実行される脆弱性 (MS12-027)(CVE-2012-0158)に関する検証レポート

2012/4/27
NTT データ先端技術株式会社
辻 伸弘
渡邊 尚道

【概要】
Windows コモンコントロールに、任意のコードが実行される脆弱性が存在します。
Windows コモンコントールとは、MSCOMCTL.OCX ファイル内に含まれる ActiveX コントロールです。
このコントロールは、Microsoft Office 等の複数のアプリケーションが共有コンポーネントとして、使用しているため、複数の製品に影響があります。

この脆弱性により、攻撃者が細工した Office ファイルを添付した電子メールを送信し、攻撃対象ユーザにファイルを開かせることでローカルユーザと同じ権限を奪取される危険性があります。今回、この Windows の脆弱性（MS12-027）（CVE-2012-0158）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】
- Microsoft Office 2003 Service Pack 3
- Microsoft Office 2003 Web コンポーネント Service Pack 3
- Microsoft Office 2007 Service Pack 2
- Microsoft Office 2007 Service Pack 3
- Microsoft Office 2010 (32 ビット版)
- Microsoft Office 2010 Service Pack 1 (32 ビット版)
- Microsoft SQL Server 2000 Analysis Services Service Pack 4
- Microsoft SQL Server 2000 Service Pack 4
- Microsoft SQL Server 2005 Express Edition with Advanced Services Service Pack 4
- Microsoft SQL Server 2005 for 32-bit Systems Service Pack 4
- Microsoft SQL Server 2005 for Itanium-based Systems Service Pack 4
- Microsoft SQL Server 2005 for x64-based Systems Service Pack 4
- Microsoft SQL Server 2008 for 32-bit Systems Service Pack 2
- Microsoft SQL Server 2008 for 32-bit Systems Service Pack 3
- Microsoft SQL Server 2008 for x64-based Systems Service Pack 2
- Microsoft SQL Server 2008 for x64-based Systems Service Pack 3
- Microsoft SQL Server 2008 for Itanium-based Systems Service Pack 2
- Microsoft SQL Server 2008 for Itanium-based Systems Service Pack 3
- Microsoft SQL Server 2008 R2 for 32-bit Systems
- Microsoft SQL Server 2008 R2 for x64-based Systems
- Microsoft SQL Server 2008 R2 for Itanium-based Systems
- Microsoft BizTalk Server 2002 Service Pack 1
- Microsoft Commerce Server 2002 Service Pack 4
- Microsoft Commerce Server 2007 Service Pack 2
- Microsoft Commerce Server 2009
- Microsoft Commerce Server 2009 R2
- Microsoft Visual FoxPro 8.0 Service Pack 1
- Microsoft Visual FoxPro 9.0 Service Pack 2
- Visual Basic 6.0 ランタイム

【対策案】

Microsoft 社より、この脆弱性を修正するプログラム（MS12-027）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 社では以下のように ActiveX コントロールを実行されないようにするという回避策を提示しております。速やかに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。

① 次のコンテンツで、ファイル名 Disable_MSCOMCTL.reg としてテキスト ファイルを作成

```
Windows Registry Editor Version 5.00[HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Internet
Explorer¥ActiveX Compatibility¥{C74190B6-8589-11d1-B16A-00C0F0283628}]"Compatibility
Flags"=dword:00000400[HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Microsoft¥Internet
Explorer¥ActiveX Compatibility¥{C74190B6-8589-11d1-B16A-00C0F0283628}]"Compatibility
Flags"=dword:00000400[HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Internet Explorer¥ActiveX
Compatibility¥{996BF5E0-8044-4650-ADEB-0B013914E99C}]"Compatibility
Flags"=dword:00000400[HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Microsoft¥Internet
Explorer¥ActiveX Compatibility¥{996BF5E0-8044-4650-ADEB-0B013914E99C}]"Compatibility
Flags"=dword:00000400[HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Internet Explorer¥ActiveX
Compatibility¥{9181DC5F-E07D-418A-ACA6-8EEA1ECB8E9E}]"Compatibility
Flags"=dword:00000400[HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Microsoft¥Internet
Explorer¥ActiveX Compatibility¥{9181DC5F-E07D-418A-ACA6-8EEA1ECB8E9E}]"Compatibility
Flags"=dword:00000400[HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Internet Explorer¥ActiveX
Compatibility¥{bdd1f04b-858b-11d1-b16a-00c0f0283628}]"Compatibility
Flags"=dword:00000400[HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Microsoft¥Internet
Explorer¥ActiveX Compatibility¥{bdd1f04b-858b-11d1-b16a-00c0f0283628}]"Compatibility
Flags"=dword:00000400
```

② .reg ファイルをダブルクリックして、個別のシステムに適用します。
*レジストリ エディタによるレジストリの編集を誤ると、システムに重大な障害が発生する可能性があります、実施の際は、システムのバックアップを取得し、十分な検証の後、実行することを推奨します。

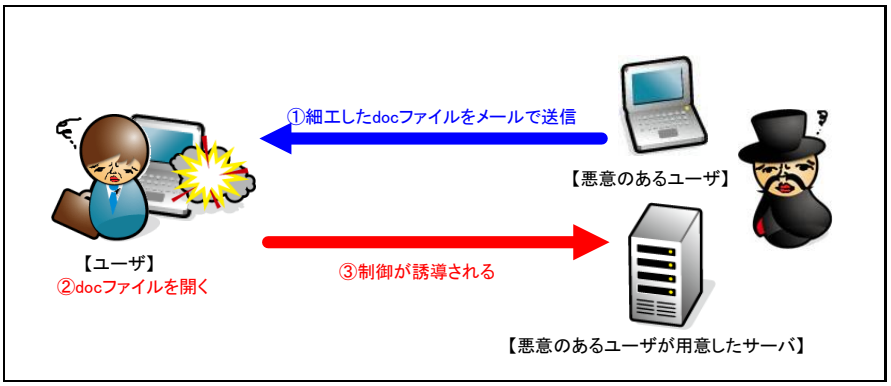
【参考サイト】

マイクロソフト セキュリティ情報 MS12-027 - 緊急
Windows コモン コントロールの脆弱性により、リモートでコードが実行される (2664258)
http://technet.microsoft.com/ja-jp/security/bulletin/MS12-027

CVE-2012-0158
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2012-0158

Microsoft Office 等の脆弱性について(MS12-027)(CVE-2012-0158)
http://www.ipa.go.jp/security/ciadr/vul/20120411-Windows.html

【検証イメージ】

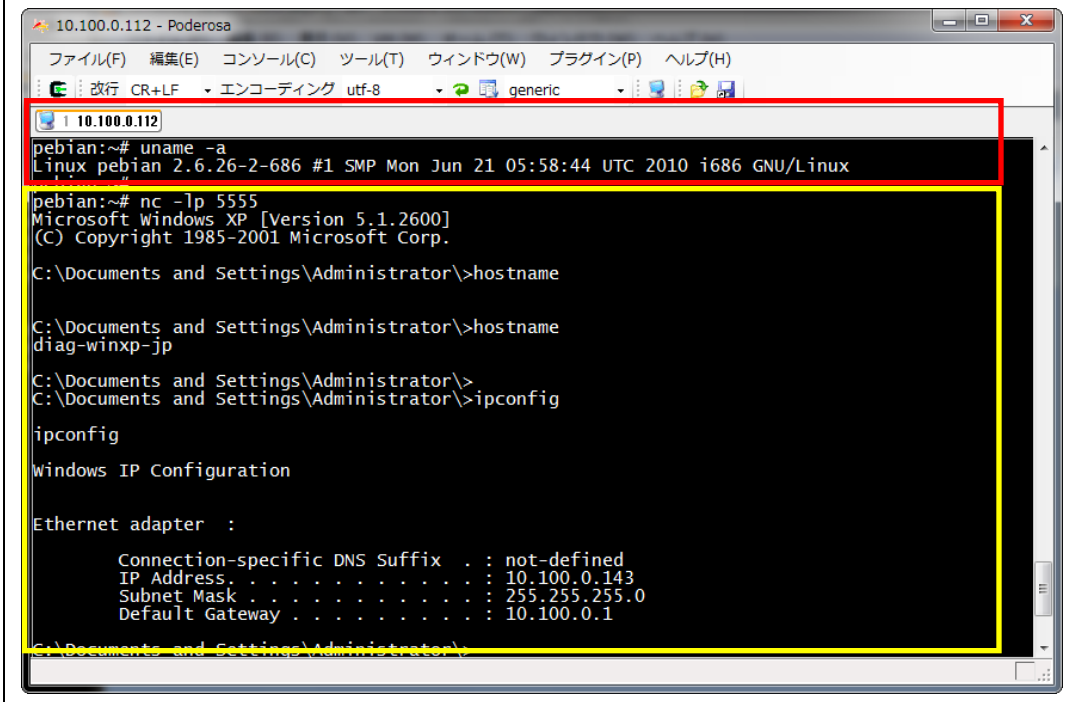


【検証ターゲットシステム】
WindowsXP SP3 Office2007 SP3

【検証概要】
ターゲットシステムにおいて、細工したワードファイルを開かせ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 5.05 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