NTTデータ・セキュリティ株式会社

Microsoft Video ActiveX コントロールの脆弱性(CVE-2008-0015)に関する検証レポート

2009/7/8
診断ビジネス部
辻 伸弘
松田 和之

【概要】

Microsoft Video ActiveX コントロールの処理に脆弱性が存在することが発見されました。
この脆弱性により、細工された Web ページの閲覧、HTML 電子メールの表示、または、電子メールの添付を開いた場合に、そのローカルユーザと同じ権限が奪取される恐れがあります。
Microsoft Video ActiveX コントロールとは、ビデオの録画・再生をするために利用されるコンポーネントであり、Internet Explorer 等で利用されています。

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、Microsoft Video ActiveX コントロール処理の脆弱性（CVE-2008-0015）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】

Windows XP Service Pack 2 および Windows XP Service Pack 3
Windows XP Professional x64 Edition Service Pack 2
Windows Server 2003 Service Pack 2
Windows Server 2003 x64 Edition Service Pack 2
Windows Server 2003 with SP2 for Itanium-based Systems

【対策案】

このレポート作成現在（2009 年 7 月 8 日)、修正プログラムはリリースされておりません。
修正プログラムのリリース、適用までは、Microsoft Video ActiveX コントロールを無効にする、Internet Explorer を利用せず脆弱性の影響を受けない代替ブラウザを使用する、または、怪しいサイトやメールの閲覧を行わないことが推奨されます。

マイクロスソフトセキュリティアドバイザリにて、回避策として Microsoft Video ActiveX コントロールを無効にするプログラムが提供されています。
http://support.microsoft.com/kb/972890

【参考サイト】

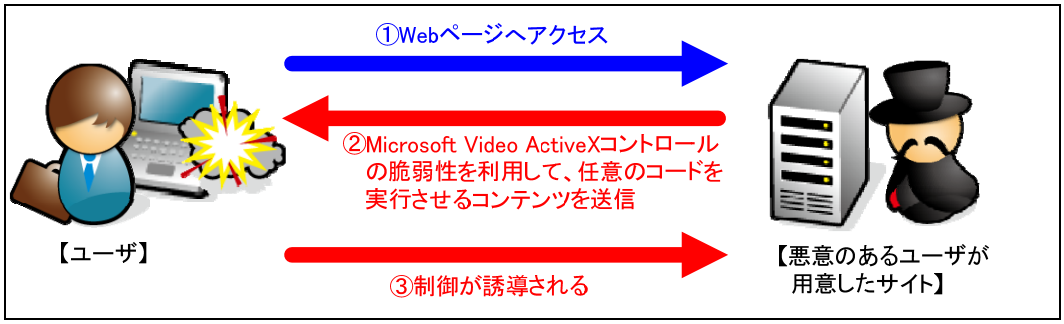
マイクロソフト セキュリティ アドバイザリ
http://support.microsoft.com/kb/972890
http://www.microsoft.com/japan/technet/security/advisory/972890.mspx

CVE - CVE-2008-0015
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0015

Copyright © 2009. NTT DATA SECURITY CORPORATION All right reserved.

NTTデータ・セキュリティ株式会社

【検証イメージ】



【検証ターゲットシステム】

Microsoft Internet Explorer 7 がインストールされた Windows XP Service Pack 3 (Version: 7.0.5730.13)

【検証概要】

ターゲットシステムに、細工した Web コンテンツをロードさ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を操作可能となります。
＊ 誘導先のシステムは CentOS 4 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（CentOS）のコマンドプロンプト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の奪取に成功した画面

```
[root@localhost ~]# nc -lp 4444
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:¥Documents and Settings¥Administrator¥デスクトップ>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter ローカル エリア接続:

        Connection-specific DNS Suffix  . : not-defined
        IP Address. . . . . . . . . . . . : 10.100.0.143
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.100.0.1

C:¥Documents and Settings¥Administrator¥デスクトップ>
```

Copyright © 2009. NTT DATA SECURITY CORPORATION All right reserved.

NTTデータ・セキュリティ株式会社

【対策案】

このレポート作成現在（2009 年 7 月 8 日）、修正プログラムはリリースされておりません。
修正プログラムのリリース、適用までは、Microsoft Video ActiveX コントロールを無効にする、Internet Explorer を利用せず脆弱性の影響を受けない代替ブラウザを使用する、または、怪しいサイトやメールの閲覧を行わないことが推奨されます。

マイクロスソフトセキュリティアドバイザリにて、回避策として Microsoft Video ActiveX コントロールを無効にするプログラムが提供されています。
http://support.microsoft.com/kb/972890

【参考サイト】

マイクロソフト セキュリティ アドバイザリ
http://support.microsoft.com/kb/972890
http://www.microsoft.com/japan/technet/security/advisory/972890.mspx

CVE - CVE-2008-0015
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0015

＊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
営業企画部
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/

Copyright © 2009. NTT DATA SECURITY CORPORATION All right reserved.