NTTデータ先端技術株式会社

Windows Media Player の MIDI ファイル処理における脆弱性(MS12-004)(CVE-2012-0003) に関する検証レポート

2012/1/30
NTT データ先端技術株式会社
辻 伸弘
渡邊 尚道

【概要】

Microsoft Windows の Windows Media Player 内にて MIDI ファイルの処理に使用されている、Windows マルチメディア ライブラリ (winmm.dll)に、任意のコードが実行される脆弱性が存在します。
winmm.dll は、Windows Media Player 等のアプリケーションが、オーディオファイルやビデオファイルを扱う際に使用されるものです。

本脆弱性は、winmm.dll が、MIDI ファイルを処理する際に、リモートコードが実行可能となる脆弱性です。

この脆弱性により、攻撃者が細工した MIDI ファイルを電子メールに添付し送信、または何らかの方法でユーザを攻撃者の Web サイトに誘導し、細工した MIDI ファイルを再生させることで、ローカルユーザと同じ権限を奪取できる危険性があります。

今回、この Windows の脆弱性 (MS12-004) (CVE-2012-0003) 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 3
-Windows XP Media Center Edition 2005 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
-Windows Vista Service Pack 2
-Windows Vista x64 Edition Service Pack 2
-Windows Server 2008 for 32-bit Systems Service Pack 2
-Windows Server 2008 for x64-based Systems Service Pack 2
-Windows Server 2008 for Itanium-based Systems Service Pack 2

【対策案】

Microsoft 社より、この脆弱性を修正するプログラム (MS12-004) 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:MIDI の解析処理を無効にします。

① 次のコマンドを昇格されたコマンド プロンプトで使用して、MIDI パーサーの元のレジストリ値を保存します。

```
regedit /e Backup.reg HKEY_CLASSES_ROOT¥CLSID¥{D51BD5A2-7548-11CF-A520-0080C77EF58A}
```

② 次のコンテンツの .reg ファイルを使用して、MIDI パーサーの登録を解除します。

```
Windows Registry Editor Version 5.00[-HKEY_CLASSES_ROOT¥CLSID¥{D51BD5A2-7548-11CF-A520-0080C77EF58A}]
```

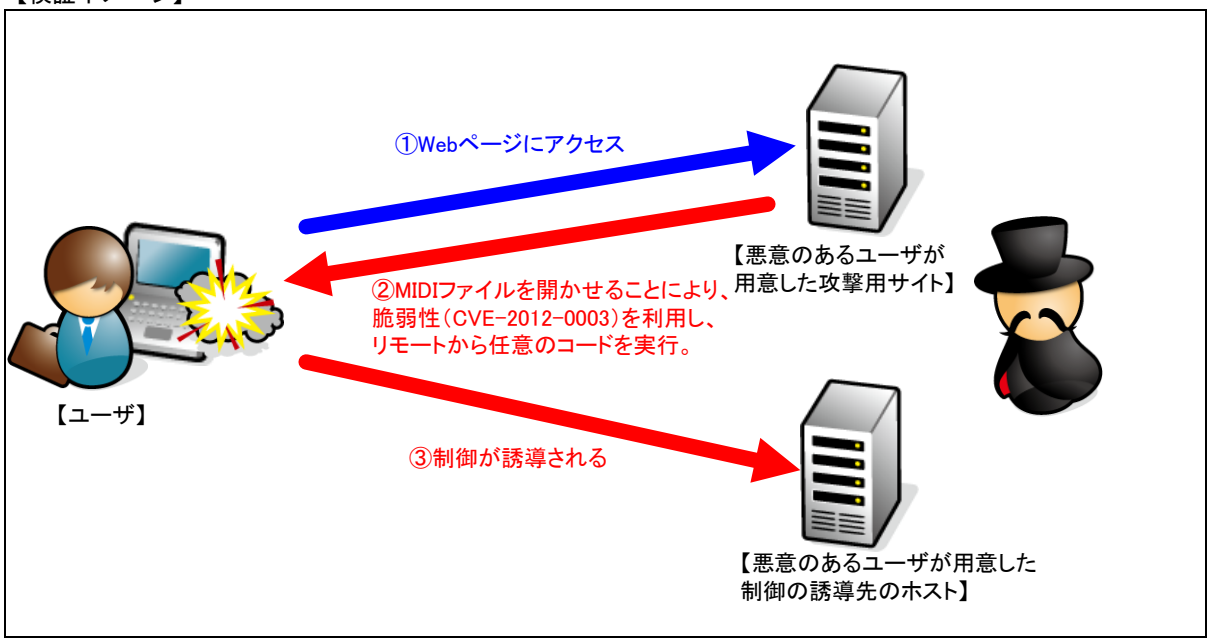
NTTデータ先端技術株式会社

【参考サイト】
マイクロソフト セキュリティ情報 MS12-004 - 緊急
Windows Media の脆弱性により、リモートでコードが実行される (2636391)
http://technet.microsoft.com/ja-jp/security/bulletin/ms12-004

CVE-2012-0003
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2012-0003

Windows Media Player の脆弱性について(MS12-004)(CVE-2012-0003)
http://www.ipa.go.jp/security/ciadr/vul/20120127-wmplayer.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、Web ページを閲覧させ、細工した MIDI ファイルを開かせることで、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。

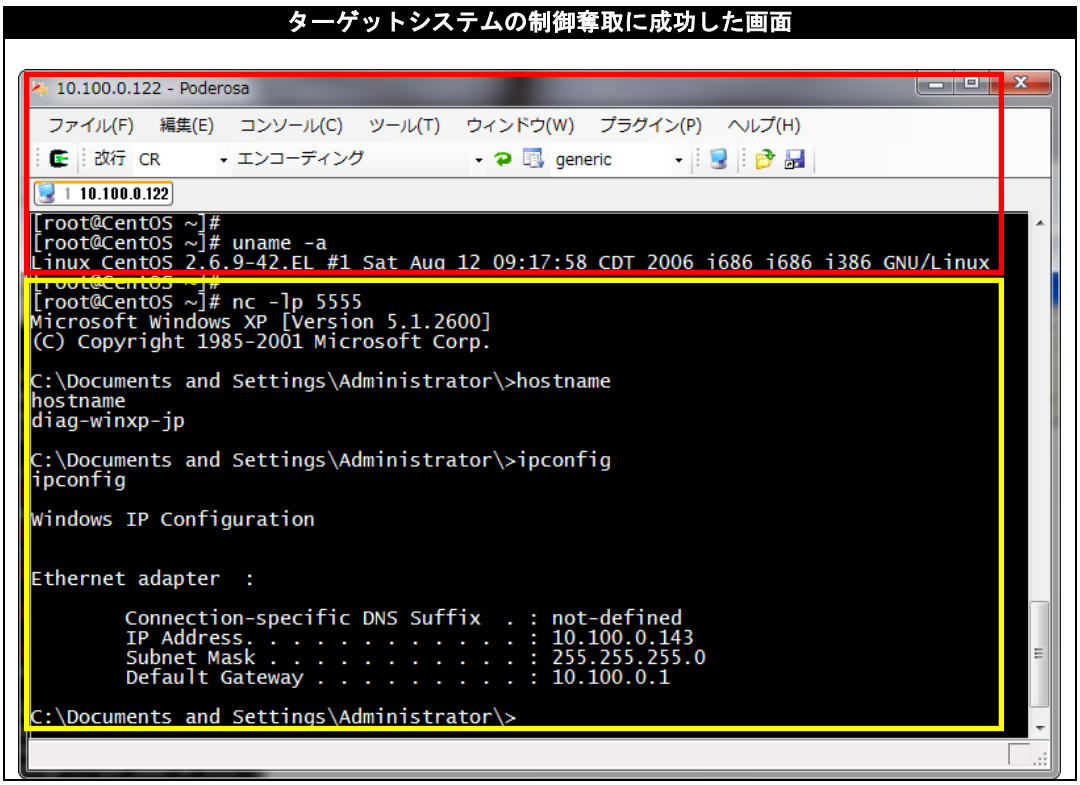
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムが操作可能となります。
** 誘導先のシステムは CentOS 4.4 です。*

NTTデータ先端技術株式会社

【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　営業企画グループ
TEL:03-5425-1954
http://security.intellilink.co.jp/