NTTデータ 先端技術株式会社

Apple QuickTime の脆弱性により、任意のコードが実行される脆弱性 (CVE-2012-0663)に関する検証レポート

2012/7/3
NTT データ先端技術株式会社
辻 伸弘
泉田 幸宏

【概要】

Windows 上で動作する Apple QuickTime に、リモートより任意のコードが実行される脆弱性が発見されました。
本脆弱性は、QuickTime が TeXML ファイル内の特定の要素を処理する際に、入力データ長を検証していないことにより発生します。TeXML ファイルは、ムービー内に表示させるテキストのスタイルを定義するためのものです。

この脆弱性により、リモートから QuickTime を実行するローカルユーザと同じ権限で任意のコードを実行される危険性があります。攻撃者は、ブラウザ経由でメディアファイルを読み込ませるように特別に細工された Web サイトにユーザを誘導することや、細工されたメディア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

この脆弱性については、Apple 社より 5 月 15 日に脆弱性が修正されたバージョンの QuickTime がリリースされております。しかしながら、攻撃を成立させるためのコードが容易に入手可能であり、かつ脆弱性に対する攻撃が容易であること、また攻撃を受けた際にシステムへの影響が大きいことから、今回、この QuickTime の脆弱性（CVE-2012-0663）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】

-Apple QuickTime 7.7.2 以前

【対策案】

Apple 社より、この脆弱性を修正するバージョンがリリースされています。
当該脆弱性が修正されたバージョンにアップデートしていただくことを推奨いたします。
-Apple QuickTime 7.7.2

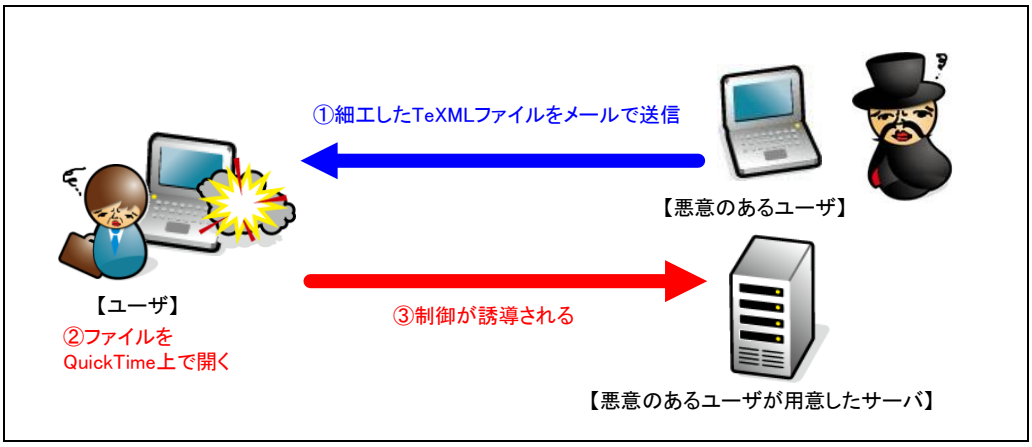
【参考サイト】

CVE-2012-0663
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0663

Apple セキュリティアップデート (Apple Security Update)
http://support.apple.com/kb/HT1222?viewlocale=ja_JP

JVNDB-2012-002428
Windows 上で稼働する Apple QuickTime におけるスタックベースのバッファオーバーフローの脆弱性
http://jvndb.jvn.jp/ja/contents/2012/JVNDB-2012-002428.html

【検証イメージ】



【検証ターゲットシステム】
Windows XP SP3
QuickTime バージョン 7.6.1292

【検証概要】
ターゲットシステム上の QuickTime で、悪意のあるユーザが作成した TeXML 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。

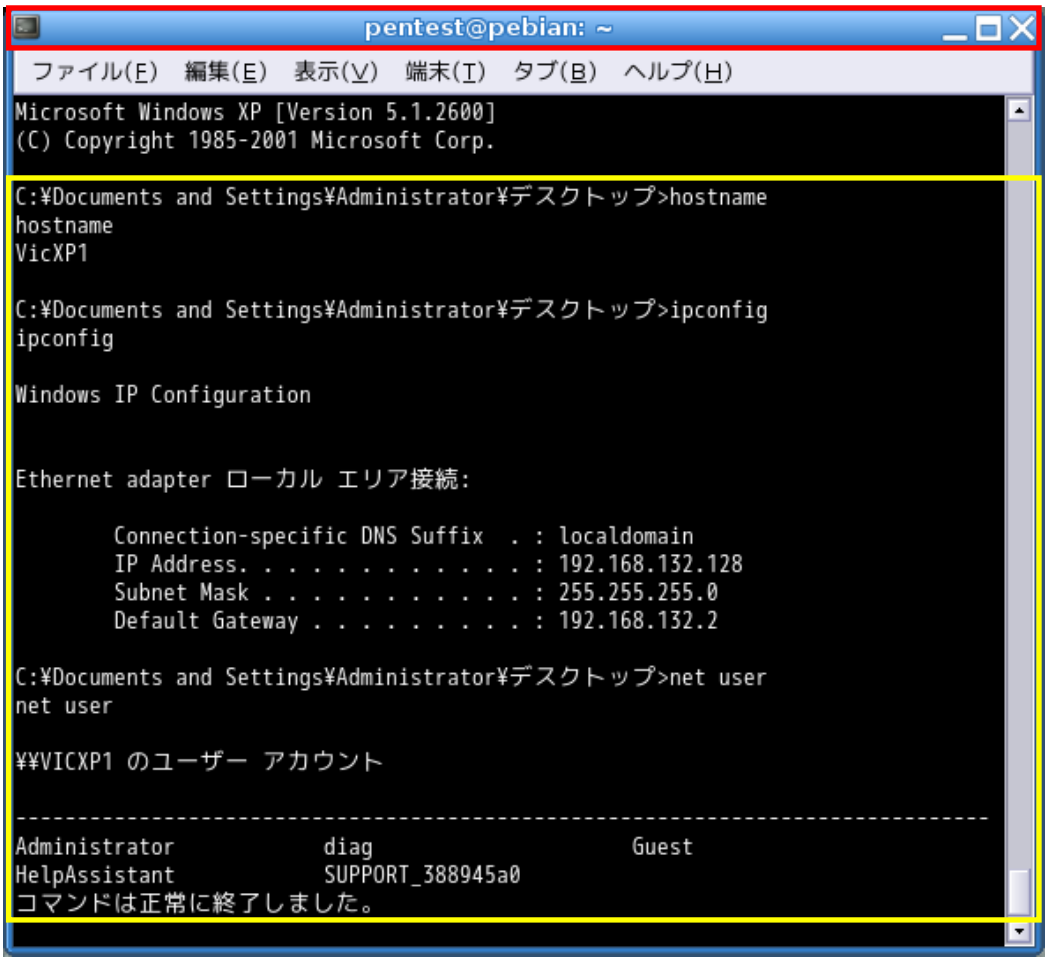
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムが操作可能となります。
** 誘導先のシステムは Debian です。*

【検証結果】

下図は、攻撃後の誘導先のシステム画面です。

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