

## Apple QuickTime の TeXML ファイルの処理の不備により任意のコードが実行される脆弱性 (CVE-2012-3752)に関する検証レポート

2012/11/27

NTT データ先端技術株式会社

辻 伸弘

小田切 秀暁

### 【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 style 要素を処理する際に発生します。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が実行される危険性があります。攻撃者が、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。

今回、この QuickTime の脆弱性 (CVE-2012-3752) 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】

影響を受ける可能性が報告されているのは次の通りです。

- Apple QuickTime 7.7.2 およびそれ以前のバージョン

### 【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 7.7.3

### 【参考サイト】

CVE-CVE-2012-3752

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3752>

QuickTime 7.7.3 のセキュリティコンテンツについて

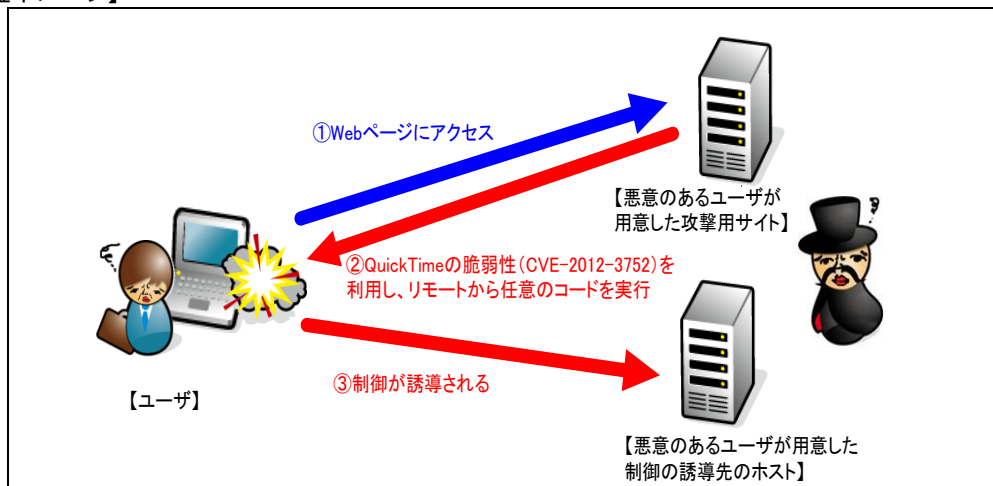
[http://support.apple.com/kb/HT5581?viewlocale=ja\\_JP](http://support.apple.com/kb/HT5581?viewlocale=ja_JP)

JVNDB-2012-005298

Apple QuickTime におけるバッファオーバーフローの脆弱性

<http://jvndb.jvn.jp/ja/contents/2012/JVNDB-2012-005298.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 7.7.2

**【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 Ubuntu です。

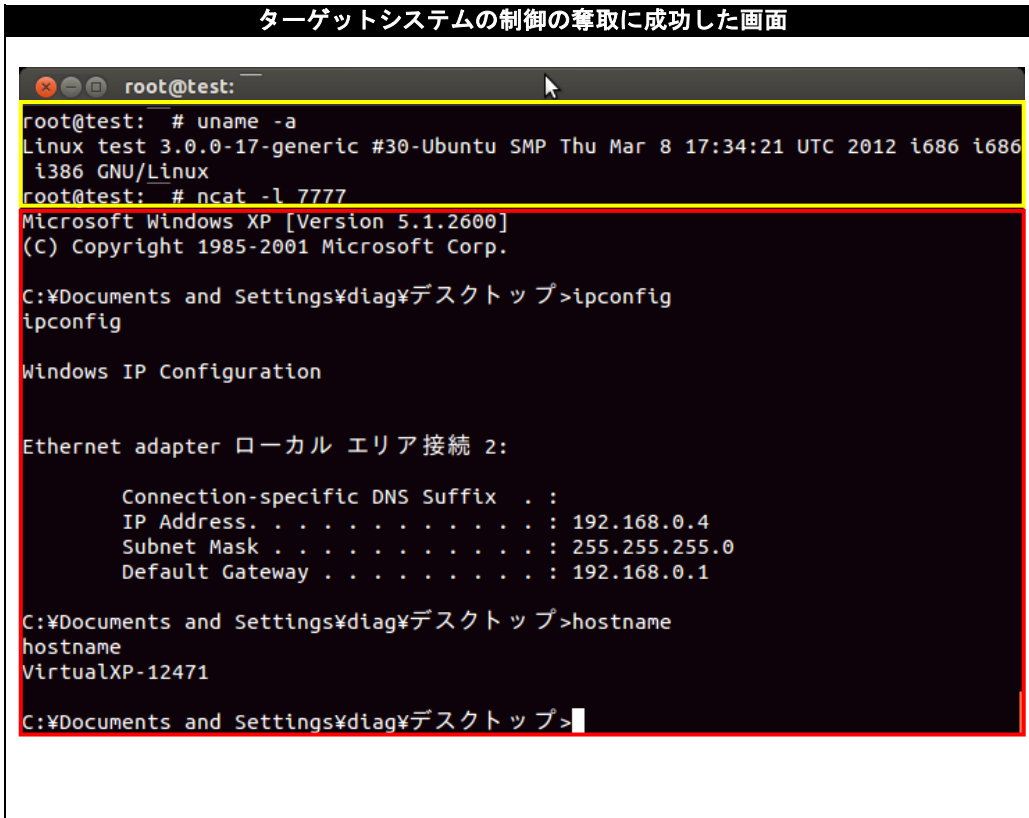
**【検証結果】**

下図の黄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 (Ubuntu) のコンソール上にターゲットシステム (Windows XP SP3) のプロンプトが表示されています。

赤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@test: # uname -a
Linux test 3.0.0-17-generic #30-Ubuntu SMP Thu Mar 8 17:34:21 UTC 2012 i686 i686
i386 GNU/Linux
root@test: # ncat -l 7777
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

Windows IP Configuration

Ethernet adapter ローカル エリア接続 2:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.0.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

C:¥Documents and Settings¥diag¥デスクトップ>hostname
hostname
VirtualXP-12471

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

\* 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

TEL:03-5859-5422

<http://security.intellilink.co.jp>