NTTデータ・セキュリティ株式会社

Apple QuickTime
RTSP Content-Type ヘッダ オーバフローの脆弱性に関する検証レポート

2007/11/27
NTT データ・セキュリティ株式会社
辻 伸弘
松田 和之

【概要】

Apple 社の QuickTime が使用する RTSP（Real Time Streaming Protocol）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 RTSP ストリームを含む 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、ローカルユーザと同じ権限の制御が奪取される恐れがあります。

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、この脆弱性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】

QuickTime 7.3 がインストールされたシステム
※このレポート作成現在（2007 年 11 月 27 日）の情報では、バージョン 7.3 以外でも影響を受ける可能性があります。

【対策案】

このレポート作成現在（2007 年 11 月 27 日）、ベンダーより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、怪しいサイトやメールの閲覧を行わない、または、RTSP のブロック、ブラウザでの機能制限など QuickTime を無効化することが推奨されます。

【参考サイト】

Apple QuickTime RTSP Content-Type header stack buffer overflow
http://www.kb.cert.org/vuls/id/659761

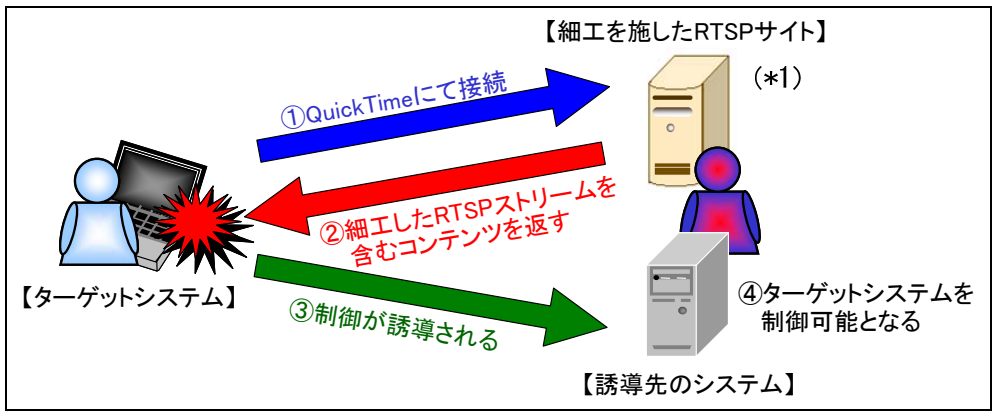
Apple QuickTime RTSP "Content-Type" Header Buffer Overflow
http://secunia.com/advisories/27755/

＊各規格名、会社名、団体名、サービス名等は、各社の商標または登録商標です。

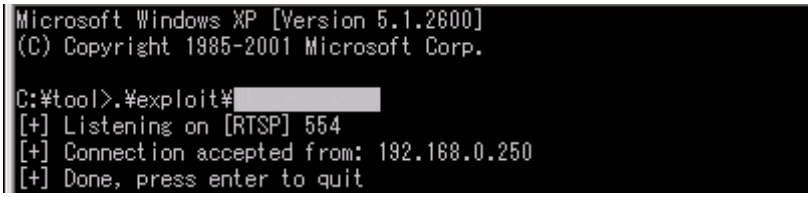
【備考】

QuickTime は iTunes のコンポーネントでもあるため、iTunes もこの脆弱性の影響を受けます。

【検証イメージ】



(*1) 細工を施した RTSP サイトの待ち受け画面



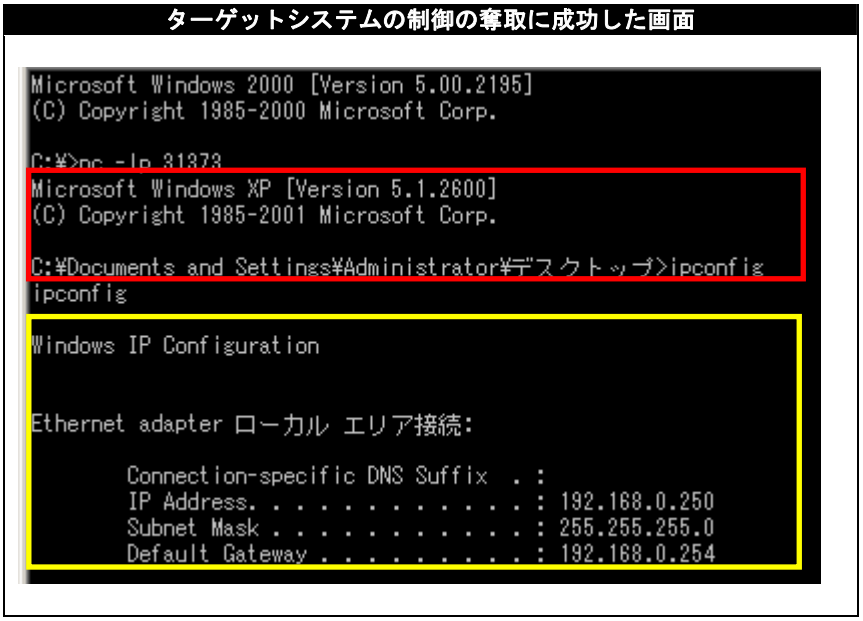
【検証ターゲットシステム】
QuickTime 7.3 がインストールされた Windows XP Service Pack 2

【検証概要】
ターゲットシステムに、細工した RTSP ストリームを含む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 Windows 2000 Professional Service Pack 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（Windows 2000）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おります。
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おります。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



【対策案】

このレポート作成現在（2007 年 11 月 27 日）、ベンダーより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、怪しいサイトやメールの閲覧を行わない、または、RTSP のブロック、ブラウザでの機能制限など QuickTime を無効化することが推奨されます。

【参考サイト】

Apple QuickTime RTSP Content-Type header stack buffer overflow
http://www.kb.cert.org/vuls/id/659761

Apple QuickTime RTSP "Content-Type" Header Buffer Overflow
http://secunia.com/advisories/27755/

＊各規格名、会社名、団体名、サービス名等は、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/