NTTデータ・セキュリティ株式会社

Windows の DLL 読み込みの欠陥により任意のコードが実行可能な脆弱性に関する検証レポート

2010/8/25
NTT データ・セキュリティ株式会社
辻 伸弘
小田切 秀暁

【概要】

Windows の DLL(Dynamic Link Library)の読み込みに、設計上の欠陥が存在します。
この脆弱性は DLL が読み込まれる際に、適切な順序で検索されないことに起因します。これにより、リモートから Binary Planting(バイナリコードの植え付け)または DLL Preloading Attack(DLL のプリロード攻撃)と呼ばれる攻撃が実行される可能性があります。

例えば、アプリケーションはパス名「C:¥Program Files¥Common Files¥system¥dllname.dll」を使用する代わりにそのカレントディレクトリに存在する「dllname.dll」を読み込むことが可能です。不正なライブラリのコピーがカレントディレクトリに存在するとアプリケーションはライブラリを完全なパスで検索せずにカレントディレクトリを検索するため不正なライブラリが読み込まれます。

悪用されるケースとしては、Windows ファイル共有や WebDAV などのリモートファイル共有が挙げられます。ブラウザによる閲覧をトリガとして不正な WebDav サーバへと誘導し、細工したファイルを閲覧させるという攻撃方法が考えられます。

この脆弱性により、Web ページの閲覧などで、ローカルユーザと同じ権限が奪取される危険性があります。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、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アプリケーション】

現在、Microsoft 社は、当該脆弱性の影響を受けるアプリケーションを調査中です。また、影響を受けるのは Microsoft 製品に限らず、別のメーカーの製品でも Windows 上で動作するアプリケーションなら影響を受ける恐れがあります。

【対策案】

このレポート作成現在（2010 年 8 月 25 日）修正プログラムはリリースされていません。
Microsoft 社は以下の回避策を提示しています。

- WebDAV およびリモートのネットワーク共有からのライブラリのロードを無効にする
- WebClient サービスを無効にする
- TCP ポート 139 および 445 をファイアウォールでブロックする

詳細および回避策の影響については
「マイクロソフト セキュリティ アドバイザリ (2269637)」の「回避策」を参照ください。
http://www.microsoft.com/japan/technet/security/advisory/2269637.mspx

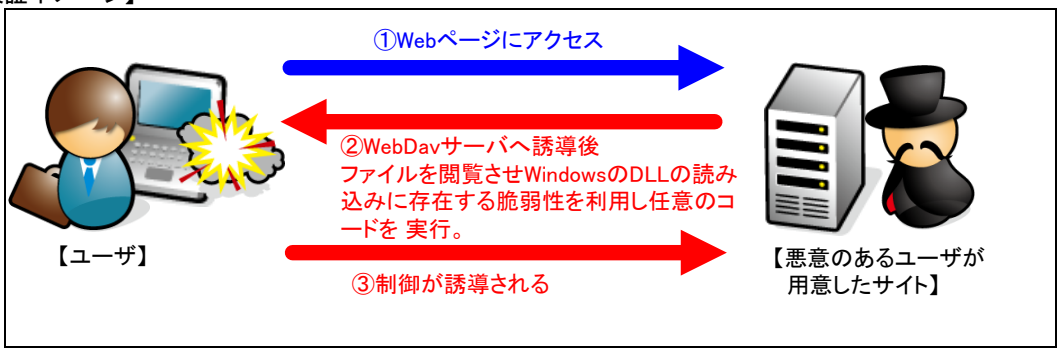
【参考サイト】

マイクロソフト セキュリティ アドバイザリ (2269637)
安全でないライブラリのロードにより、リモートでコードが実行される
http://www.microsoft.com/japan/technet/security/advisory/2269637.mspx

Copyright © 2010. 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】

Windows XP SP3（2010 年 8 月 25 日時点にリリースされているすべての修正プログラムを適用済み）

【検証概要】

ターゲットシステムに、Web ブラウザを通じて、細工した WebDAV サーバへ誘導し任意のファイルをダウンロードさせます。ユーザにダウンロードさせたファイルに関連付けられたアプリケーションを実行させることで、今回の脆弱性を利用し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 Debian GNU/Linux 5.05 です。

【検証結果】

下図が示すように、誘導先のコンピュータ（Debian GNU/Linux 5.05）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。
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

＊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
企画部　広報グループ
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/

Copyright © 2010. NTT DATA SECURITY CORPORATION All right reserved.