NTTデータ先端技術株式会社

Microsoft Office Excel における変数初期化処理の脆弱性 (CVE-2011-0105, MS11-021)に関する検証レポート

2011/11/14
NTT データ先端技術株式会社
辻　伸弘
小松　徹也

【概要】

Microsoft 社の Office 製品である Excel に、リモートから任意のコードを実行可能な既知の脆弱性(CVE-2011-0105)が存在します。
この脆弱性は Excel の変数初期化処理に存在します。Excel ファイルを解析中に正しく変数を初期化しないことから、バッファオーバーフローを引き起こす可能性があります。
この脆弱性により、電子メールの添付ファイルやメッセンジャーのメッセージ内のリンクをクリックさせて、ユーザを攻撃者の Web サイトに誘導し、細工した Excel ファイルの閲覧させることにより、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、この Excel の脆弱性(CVE-2011-0105)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】

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。
*Microsoft Office XP Service Pack 3 - Microsoft Excel 2002 Service Pack 3
*Microsoft Office 2003 Service Pack 3 - Microsoft Excel 2003 Service Pack 3
*Microsoft Office 2007 Service Pack 2 - Microsoft Excel 2007 Service Pack 2
*Microsoft Office 2010 - Microsoft Excel 2010
*Microsoft Office 2004 for Mac
*Microsoft Office 2008 for Mac
*Microsoft Office for Mac 2011
*Open XML File Format Converter for Mac
*Microsoft Excel Viewer Service Pack 2
*Word/Excel/PowerPoint 2007 ファイル形式用 Microsoft Office 互換機能パック 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(MS11-021)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。

【参考サイト】

CVE-2011-0105
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0105

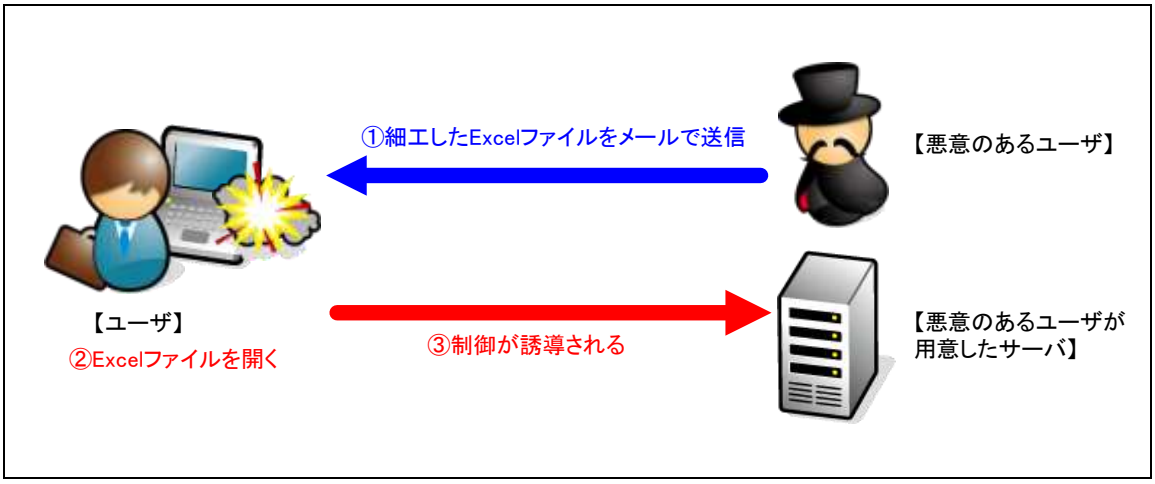
マイクロソフト セキュリティ情報 MS11-021 - 重要
Microsoft Excel の脆弱性により、リモートでコードが実行される (2489279)
http://technet.microsoft.com/ja-jp/security/bulletin/ms11-021

複数の Microsoft 製品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/2011/JVNDB-2011-001484.html

NTTデータ先端技術株式会社

【検証イメージ】

【CVE-2011-0105】



【検証ターゲットシステム】

Microsoft Windows XP SP3 および Microsoft Excel 2007 SP2

【検証概要】

ターゲットシステムに細工された Excel ファイルを閲覧させ、脆弱性を利用した攻撃コードを実行す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に誘導し、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の操作が可能となります。

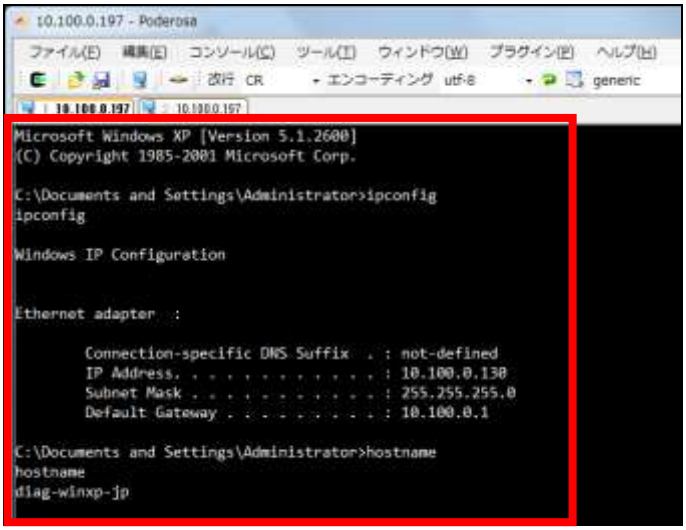
【検証結果】

下図が示すように、誘導先のコンピュータ（Linux）上にターゲットシステム（Windows XP）の情報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。

NTTデータ先端技術株式会社

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/