SoftBank Technology

ソフトバンク・テクノロジー株式会社

脆弱性調査レポート

Windows OLE の脆弱性によりリモートより任意のコードが実行される脆弱性(MS14-064)(CVE-2014-6332, CVE-2014-6352)に関する調査レポート

【概要】

Windows OLE*に複数の脆弱性があるため、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。

*OLE(Object Linking and Embedding):

複数のデータや機能が含まれた複合データを、一つのアプリケーションで編集を可能とするテクノロジです。例えば、これにより Word に埋め込まれた Excel スプレッドシートを Excel を起動せずに、Word 上で編集することが可能となります。

上記の脆弱性により、2種類の脆弱性(CVE-2014-6332 と CVE2014-6352)が公開されています。

・CVE-2014-6332 について

Windows OLE の OleAut32.dll ライブラリが SAFEARRAY オブジェクトのサイズのエラーを検証する際の処理に不具合があるため、Internet Explorer Enhanced Protected Mode (EPM) サンドボックスや Enhanced Mitigation Experience Toolkit (EMET) をバイパスすることが可能です。このため、攻撃者は VBScript を使用して細工した Web ページに、攻撃対象者を誘導することにより、攻撃対象者の Internet Explorer を実行している権限を奪うことが可能となります。

・CVE-2014-6352 について

攻撃者は、細工した OLE オブジェクトを含む Office ファイルを作成し、そのファイルが含まれるサイトに攻撃対象者を誘導しファイルを開かせたり、電子メールにファイルを添付して送信し攻撃対象者に開かせる等の行為により、攻撃対象者がファイルを開いた際の実行権限にて任意のコードを実行することが可能です。

今回、Microsoft が提供している更新プログラム(MS14-064)の修正対象となっている、二つの脆弱性(CVE-2014-6332 と CVE-2014-6352)について検証を行いました。

【影響を受ける可能性があるシステム】

・CVE-2014-6332

- Windows Server 2003 Service Pack 2
- Windows Server 2003 x 64 Edition Service Pack 2
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 2

- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for Itanium-based Systems Service Pack 2
- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
- Windows 8 for 32-bit Systems
- Windows 8 for x64-based Systems
- Windows 8.1 for 32-bit Systems
- Windows 8.1 for x64-based Systems
- Windows Server 2012
- Windows Server 2012 R2
- Windows RT
- Windows RT 8.1
- Windows Server 2008 for 32-bit Systems Service Pack 2(Server Core インストール)
- Windows Server 2008 for x64-based Systems Service Pack 2(Server Core インストール)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1(Server Core インストール)
- Windows Server 2012(Server Core インストール)
- Windows Server 2012 R2(Server Core インストール)

・CVE-2014-6352

- Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for Itanium-based Systems Service Pack 2
- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
- Windows 8 for 32-bit Systems
- Windows 8 for x64-based Systems
- Windows 8.1 for 32-bit Systems
- Windows 8.1 for x64-based Systems
- Windows Server 2012
- Windows Server 2012 R2
- Windows RT
- Windows RT 8.1

【対策案】

Microsoft 社より、この脆弱性を修正する更新プログラム（MS14-064）がリリースされています。
当該脆弱性を修正する更新プログラムを適用していただくことを推奨いたします。

CVE-2014-6332 の脆弱性については、回避策は確認されておりません。上記の更新プログラム（MS14-064)の適用を推奨します。

CVE-2014-6352 の脆弱性については、更新プログラムを適用しない場合の回避策として、以下の方法が提案されています。

・Fix it を導入する
・ユーザアカウント制御(UAC)を有効にする
・EMET5.0 の Attack Surface Reduction 機能を使用する

【参考サイト】

- Windows OLE の脆弱性により、リモートでコードが実行される (3011443)

・CVE-2014-6332

- JVNVU#96617862 Microsoft Windows OLE ライブラリに任意のコード実行が可能な脆弱性
- 複数の Microsoft 製品の OLE における任意のコードを実行される脆弱性
- CVE-2014-6332

・CVE-2014-6352

- マイクロソフト セキュリティ アドバイザリ 3010060 Microsoft OLE の脆弱性により、リモートでコードが実行される
- 2014 年 10 月 Microsoft OLE の未修正の脆弱性に関する注意喚起
- 更新：Microsoft Windows の脆弱性対策について(CVE-2014-6352)
- CVE-2014-6352

【検証概要】(CVE-2014-6332)

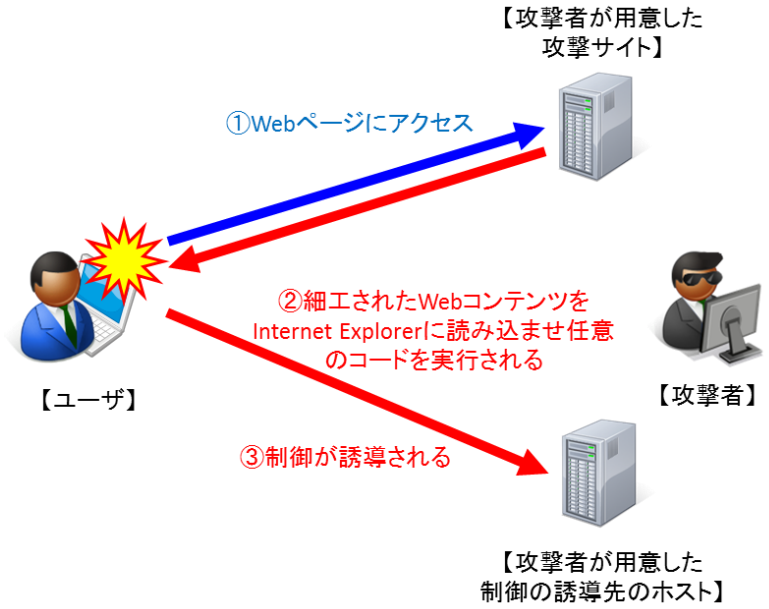
脆弱性の存在するターゲット PC より、攻撃者が作成した細工された応答を返すサーバにアクセスすることで脆弱性を利用した攻撃を行い、攻撃者が用意した制御の誘導先のホストの指定ポートにコネクトバックさせ、結果、シェルを奪取するというものです。これにより、リモートからターゲット PC の操作が可能となります。

【検証ターゲットシステム】(CVE-2014-6332)

Windows 7 Enterprise SP1 日本語版

Internet Explorer10 日本語版

【検証イメージ】(CVE-2014-6332)

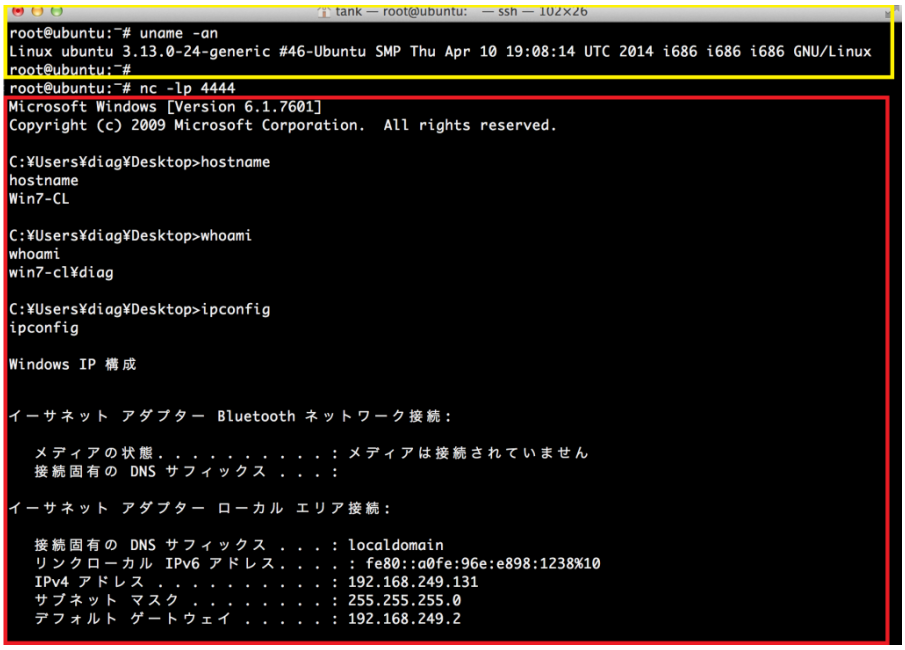


【検証結果】(CVE-2014-6332)

攻撃者が用意した Web サイトに、攻撃ターゲット PC から Internet Explorer 使い、アクセスします。

下図の様に、Internet Explorer セキュリティのダイアログが表示されますが「許可する」ボタンを押すと、脆弱性コードが攻撃ターゲット PC にて実行されます。

下図は、攻撃後の誘導先のコンピュータ(Ubuntu)の画面です。黄線で囲まれている部分は、誘導先のコンピュータのホスト情報です。一方、赤線で囲まれている部分は、ターゲット PC(Windows 7)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 PC の制御を奪うことに成功しました。



【検証概要】(CVE-2014-6352)

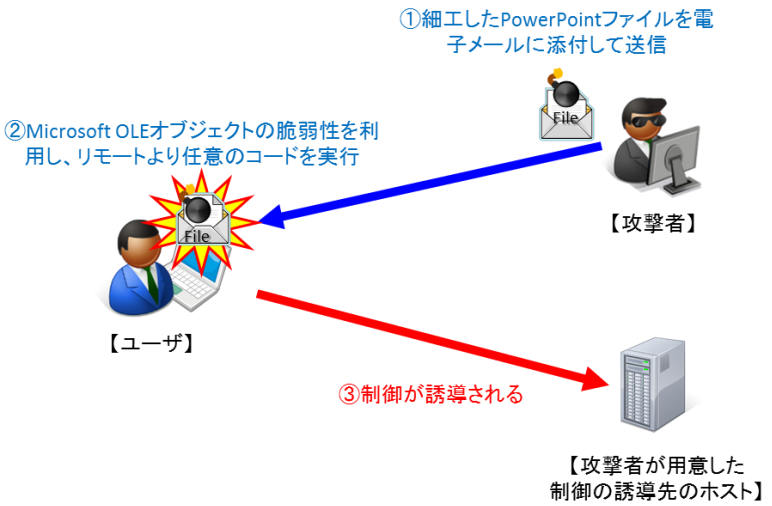
脆弱性が存在するシステムに添付ファイル付き電子メールを送信する等をして、細工を施した PowerPoint ファイルをターゲット PC にて開きます。ターゲット PC は意図せず、攻撃者が用意した制御の誘導先ホストの指定ポートにコネクトバックするマルウェアをインストール・実行し、リモートからターゲット PC の制御が可能となります。

【検証ターゲットシステム】(CVE-2014-6352)

Windows 7 Enterprise SP1 日本語版

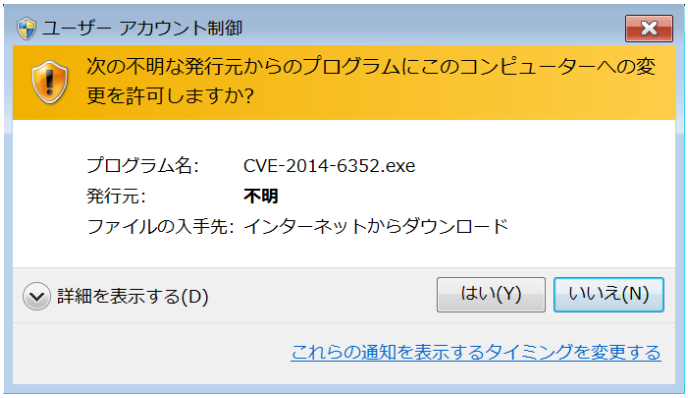
Office Professional Plus 2013 日本語版

【検証イメージ】(CVE-2014-6352)



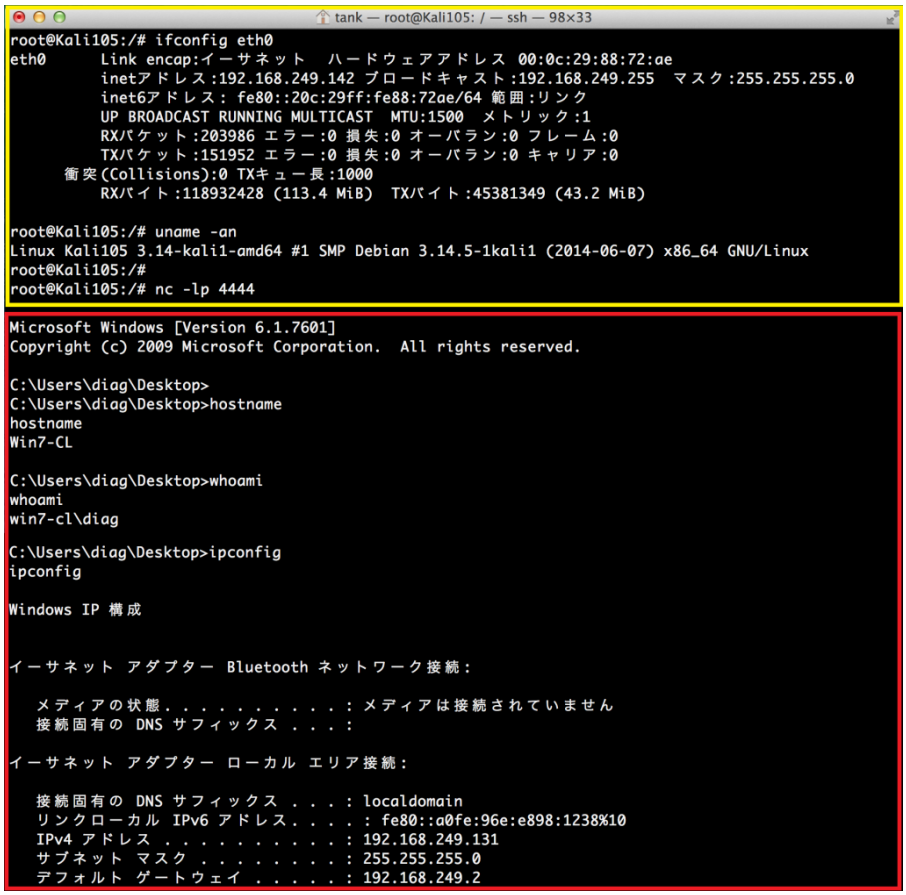
【検証結果】(CVE-2014-6352)

下図は、ターゲット PC（Windows7）にて、細工した OLE オブジェクトを含む Office ファイル(PowerPoint)ファイルを、ターゲット PC(Windows7)にて開いた時に出るダイアログです。Office ファイル(PowerPoint)ファイルを開くと、マルウェア(mal-CVE2014-6352.exe)の挙動を検知し、ユーザー アカウント制御のダイアログが表示されますが、「はい」を選択し、実行を許可すると、あらかじめ設定された任意のサーバのポートにコネクトバックします。



＊ターゲット PC に Python がインストールされている場合は、この制限も回避が可能であることを確認しております。
（今回の検証対象の、Windows 7 Enterprise SP1 日本語版 , Office Professional Plus 2013 日本語版 にて確認済）

下図は、攻撃後の誘導先のコンピュータ（Kali Linux）のターミナルの画面です。
赤線で囲まれている部分は、誘導先のコンピュータのホスト情報です。一方、黄線で囲まれている部分は、ターゲット PC（Windows7）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 PC(Windows7)の制御を奪うことに成功しました。



ソフトバンク・テクノロジー株式会社
〒160-0022 東京都新宿区新宿 6 丁目 27 番地 30 号
新宿イーストサイドスクエア 17 階
受付時間：平日 10:00～17:00

電話 03-6892-3154
メール sbt-ipsol@tech.softbank.co.jp
URL https://www.softbanktech.jp/