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

Microsoft Office およびワードパッドの脆弱性により、リモートから任意のコードが実行可能な脆弱性(CVE-2017-0199)に関する調査レポート

【概要】

Microsoft Office およびワードパッドに、リモートより任意のコードが実行可能な脆弱性（CVE-2017-0199）及び、その脆弱性を利用する攻撃コードが発見されました。

本脆弱性は、Microsoft OLE※1 における URL Moniker※2 での処理に起因する脆弱性で、細工された HTA※3 コンテンツの処理に不具合があるため生じる脆弱性です。

この脆弱性を利用し、攻撃者は細工を施した Word ファイルを電子メール等で送信し、同ファイルを受信したユーザーがそのファイルを開くことで、リモートから任意のコードを実行される等の危険性があります。

※1 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ーです。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。

※2 URL Moniker

指定した URL のリソースを、他のコンポ―ネントでも使用できるようにするサービスを提供する COM オブジェクト。

※3 HTML を動的に変化させるダイナミック HTML の機能を利用して、Windows 向けのアプリケーションを作成する技術のことです。

本レポート作成時点（2017 年 4 月 28 日）において、ベンダーより脆弱性を解決する更新プログラムがリリースされております（2017 年 4 月 11 日付）。しかしながら、攻撃を成立させるためのコードが容易に入手可能であり、かつ脆弱性に対する攻撃が容易であること、また攻撃を受けた際にシステムへの影響が大きいこと、加えてベンダーが「同脆弱性を悪用した事実を確認済み」と公表していることから、今回、この脆弱性（CVE-2017-0199）の再現性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】

- Microsoft Office 2007 Service Pack 3
- Microsoft Office 2010 Service Pack 2 (32 ビット版)
- Microsoft Office 2010 Service Pack 2 (64 ビット版)
- Microsoft Office 2013 Service Pack 1 (32 ビット版)
- Microsoft Office 2013 Service Pack 1 (64 ビット版)
- Microsoft Office 2016 (32 ビット版)

- Microsoft Office 2016 (64 ビット版)
- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for Itanium-Based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 2

【対策案】

Microsoft 社より、この脆弱性を修正する更新プログラム(KB3141529、KB3141538、KB3178710 および KB3178703)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。

【参考サイト】

- CVE-2017-0199
- CVE-2017-0199 | Microsoft Office/ワードパッド Windows API の w/リモート コード実行の脆弱性
- Microsoft OLE URL Moniker における遠隔の HTA データに対する不適切な処理

【検証概要】

添付ファイル付き電子メールを送信する等をして、脆弱性が存在するターゲットシステムが受信したと想定し、細工を施した Word ファイルをターゲットシステムにて開きます。ターゲットシステムは意図せず、攻撃者が用意した攻撃サイトにある細工された HTA コンテンツにアクセスします。今回の検証に用いた HTA コンテンツは、ターゲットシステム上から特定のサーバー、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。

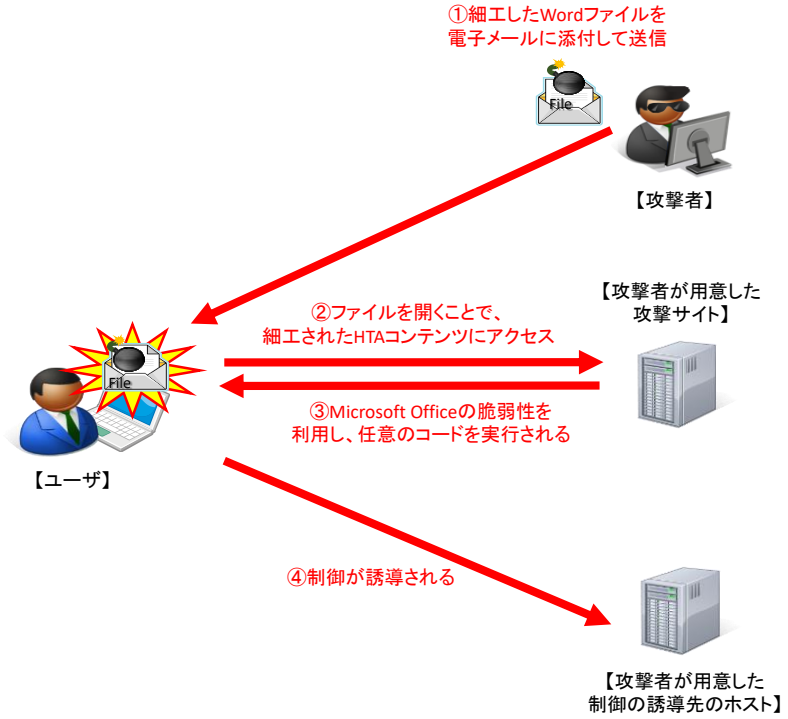
*誘導先のシステムは Linux です。

【検証ターゲットシステム】

Windows 7 Enterprise SP1 日本語版

Microsoft Office Professional Plus 2016 日本語版

【検証イメージ】

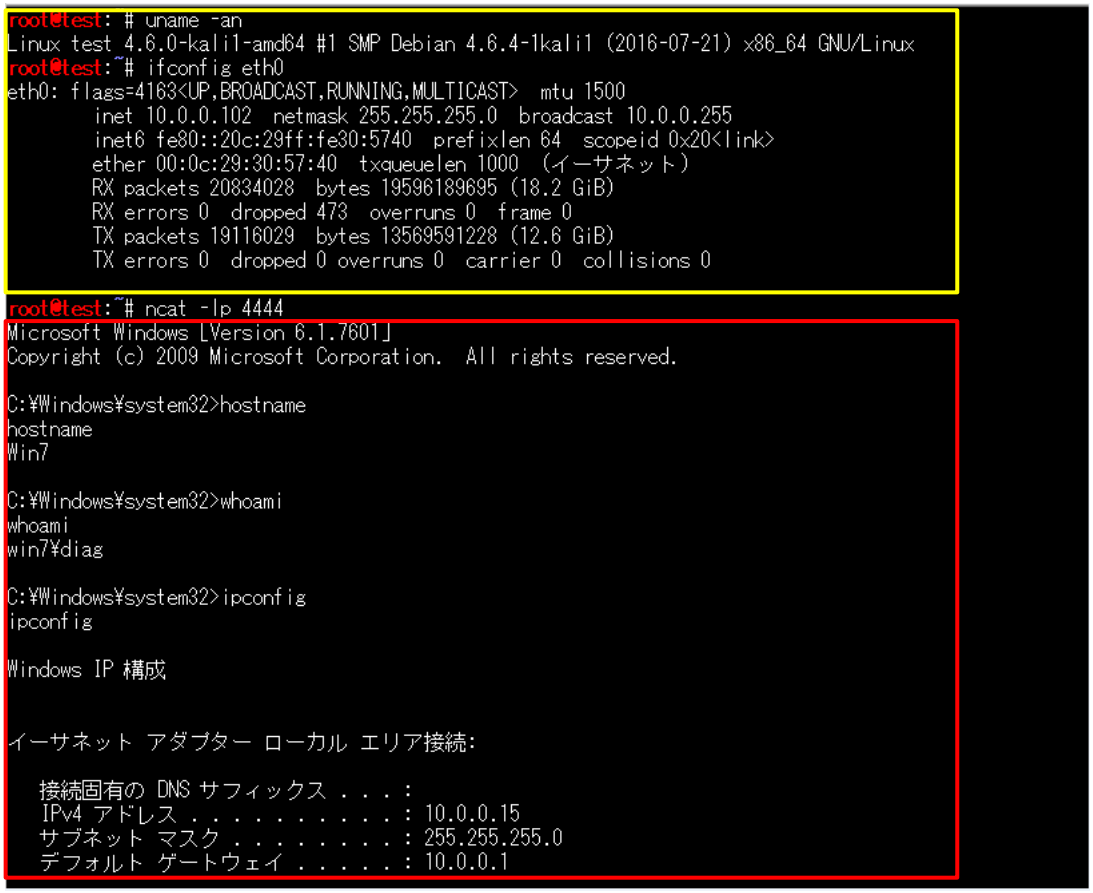


【検証結果】

下図は、誘導先のコンピュータ(Linux)の画面です。黄線で囲まれた部分は、誘導先のホストの情報です。

一方で、赤線で囲まれている部分は、ターゲットシステム(Windows7)において、ユーザーの情報、IP アドレスの情報を表示する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で任意のコマンドを実行することに成功したと判断できます。



【更新履歴】

2017 年 4 月 28 日 ： 初版公開

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/