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

Microsoft Office の数式エディターの脆弱性により、リモートから任意のコードが実行可能な脆弱性（CVE-2017-11882）に関する調査レポート

【概要】

Microsoft Office の数式エディター※1 に、リモートより任意のコードが実行可能な脆弱性（CVE-2017-11882）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、数式エディターにおける、スタックベースのバッファオーバーフローの脆弱性です。

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、同ファイル開いたユーザーの権限で任意のコードを実行される危険性があります。

※1 文書に数式を挿入するためのコンポーネント

本レポート作成（2017 年 11 月 27 日）時点において、Microsoft 社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 11 月 15 日）。しかしながら、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から、今回、この脆弱性（CVE-2017-11882）の再現性について検証を行いました。

最近のソフトウェアは、DEP(Data Execution Prevention)や ASLR(Address Space Layout Randomization)、CFG(Control Flow Guard)といった保護機能により、メモリ破損の脆弱性に対する影響の緩和を行っています。しかし、Microsoft Office の数式エディターは、最新の修正プログラムが適用された Microsoft Office 2016 のバージョンであっても、上記の保護機能が適用されないため、コード実行などの攻撃が容易となります。また、Microsoft Office の数式エディターは Out-of-process COM サーバーのため、Microsoft Office に対する保護機能、例えば、Microsoft Office プログラムに対する EMET や、Windows Defender Exploit Guard、および ASR （Windows Defender Exploit Guard Attack Surface Reduction）も適用されません。

なお、Windows 7 において、EMET の ASLR をシステム全体のレベルで「Always On」に設定している場合には、この脆弱性に対する攻撃から保護されますが、他方、Windows 8.0 から Windows 10 においては、システム全体のレベルで ASLR を設定できないため、この脆弱性に対する対策を行う必要があります。

【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-bit editions)
- Microsoft Office 2010 Service Pack 2 (64-bit editions)
- Microsoft Office 2013 Service Pack 1 (32-bit editions)
- Microsoft Office 2013 Service Pack 1 (64-bit editions)

- Microsoft Office 2016 (32-bit edition)
- Microsoft Office 2016 (64-bit edition)

【対策案】

Microsoft 社より、この脆弱性を修正する更新プログラム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。

ただちに更新プログラムを適用することが困難である場合、Microsoft 社より更新プログラムを適用しない場合の回避策として、数式エディター 3.0 を無効にする方法が提案されています。ただし、本回避策を使用した場合の影響として、数式オブジェクトが正常に機能しない場合があると報告されています。

また、Microsoft 社による公式の回避策ではありませんが、Windows 7 において、EMET の ASLR をシステム全体のレベルで「Always On」に設定することでも回避が可能です。

数式エディター 3.0 を無効にする手順は以下の通りです。

詳細は以下 Microsoft 社の Web サイトをご確認ください。

How to disable Equation Editor 3.0

1. Office のバージョンが Office2007 およびそれ以降の場合
    1. 以下のレジストリサブキーの DWORD 値を変更します。

        [HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Office¥Common¥COM Compatibility¥{0002CE02-0000-0000-C000-000000000046}]

        "Compatibility Flags"=dword:00000400

    2. 以下のエントリーを削除します。

        [HKEY_CLASSES_ROOT¥CLSID¥{0002CE02-0000-0000-C000-000000000046}]

        [HKEY_LOCAL_MACHINE¥SOFTWARE¥Classes¥Equation.3]

2. Office のバージョンが 32 ビット版の Office2007 およびそれ以降で、OS が 64 ビット版の場合
    1. 以下のレジストリサブキーの DWORD 値を変更します。

        [HKEY_LOCAL_MACHINE¥SOFTWARE¥WOW6432Node¥Microsoft¥Office¥Common¥COM Compatibility¥{0002CE02-0000-0000-C000-000000000046}]

        "Compatibility Flags"=dword:00000400

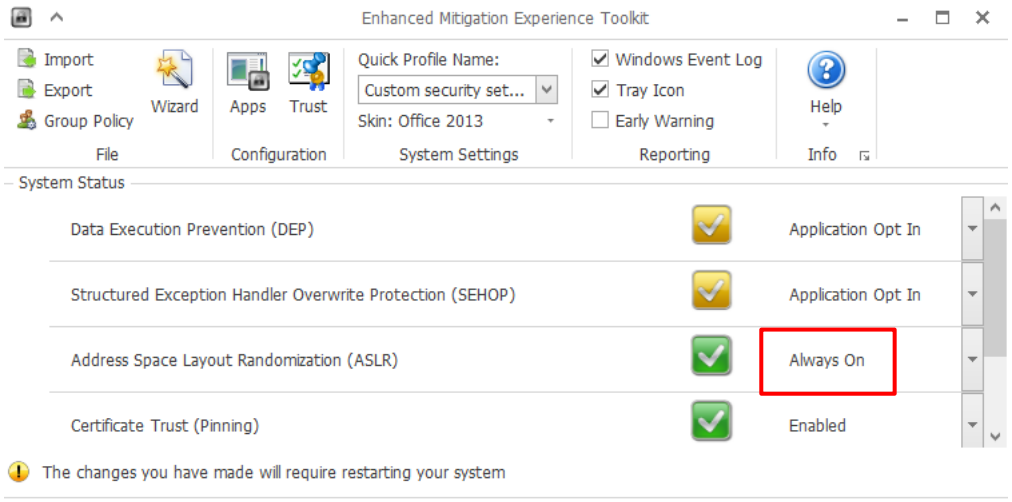
    2. 以下のエントリーを削除します。

        [HKEY_CLASSES_ROOT¥WOW6432Node¥CLSID¥{0002CE02-0000-0000-C000-000000000046}]

        [HKEY_LOCAL_MACHINE¥SOFTWARE¥Classes¥Equation.3]

EMET の ASLR をシステム全体のレベルで「Always On」に設定する手順は以下の通りです。
なお、下記は弊社環境(Windows 7 上で EMET Version5.52 を使用)の場合での設定例です。

1. 以下のレジストリサブキーの DWORD 値を変更します。
   HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥EMET
   "EnableUnsafeSettings"=dword:1
2. System Status 項目の Address Space Layout Randomization(ASLR)の設定を「Always On」に変更します。



3. コンピューターを再起動します。

【参考サイト】

- CVE - CVE-2017-11882
- CVE-2017-11882 | Microsoft Office のメモリ破損の脆弱性
- Skeleton in the closet. MS Office vulnerability you didn't know about
- Vulnerability Note VU#421280

【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。本脆弱性単体では任意のコードを実行する際に制限がありますので、まず、本脆弱性を利用して別途攻撃者が用意した HTA ファイル※2 にアクセスするコードを実行させます。その後、同 HTA ファイルによって実行形式のファイルをダウンロード、実行させます。今回の検証に用いた実行形式のファイルは、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。

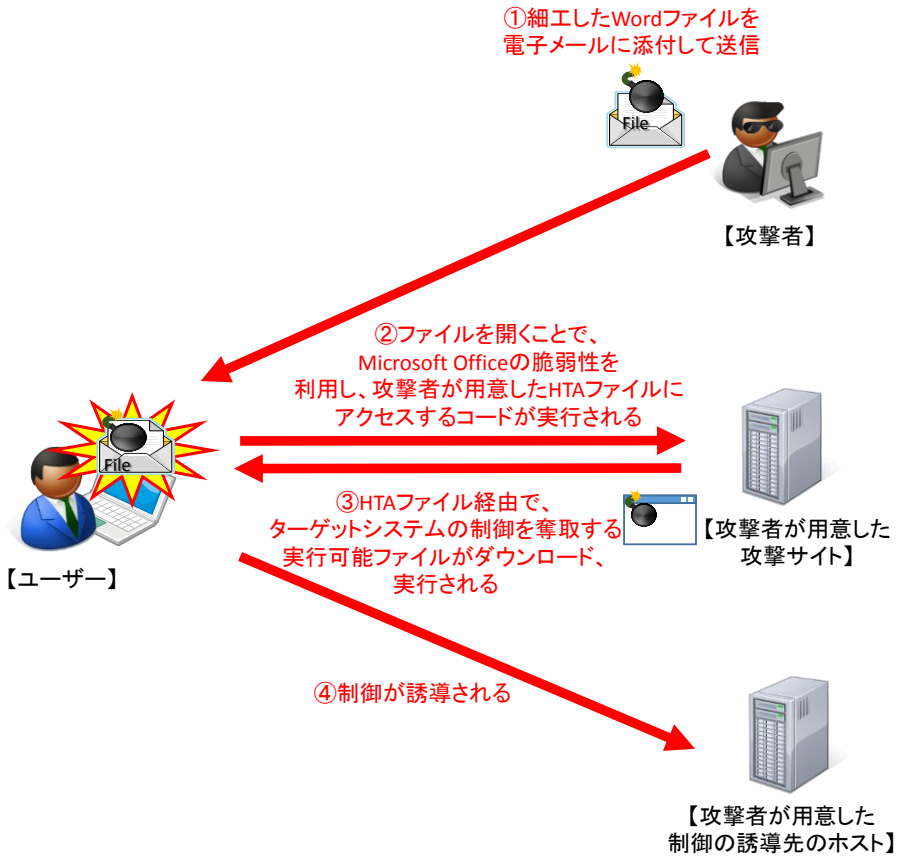
※2 HTML を動的に変化させるダイナミック HTML の機能を利用して、Windows 向けのアプリケーションを作成する技術のことです。

【検証ターゲットシステム】

Windows 7 Professional SP1　日本語版

Microsoft Office Professional Plus 2013 SP1　日本語版

【検証イメージ】

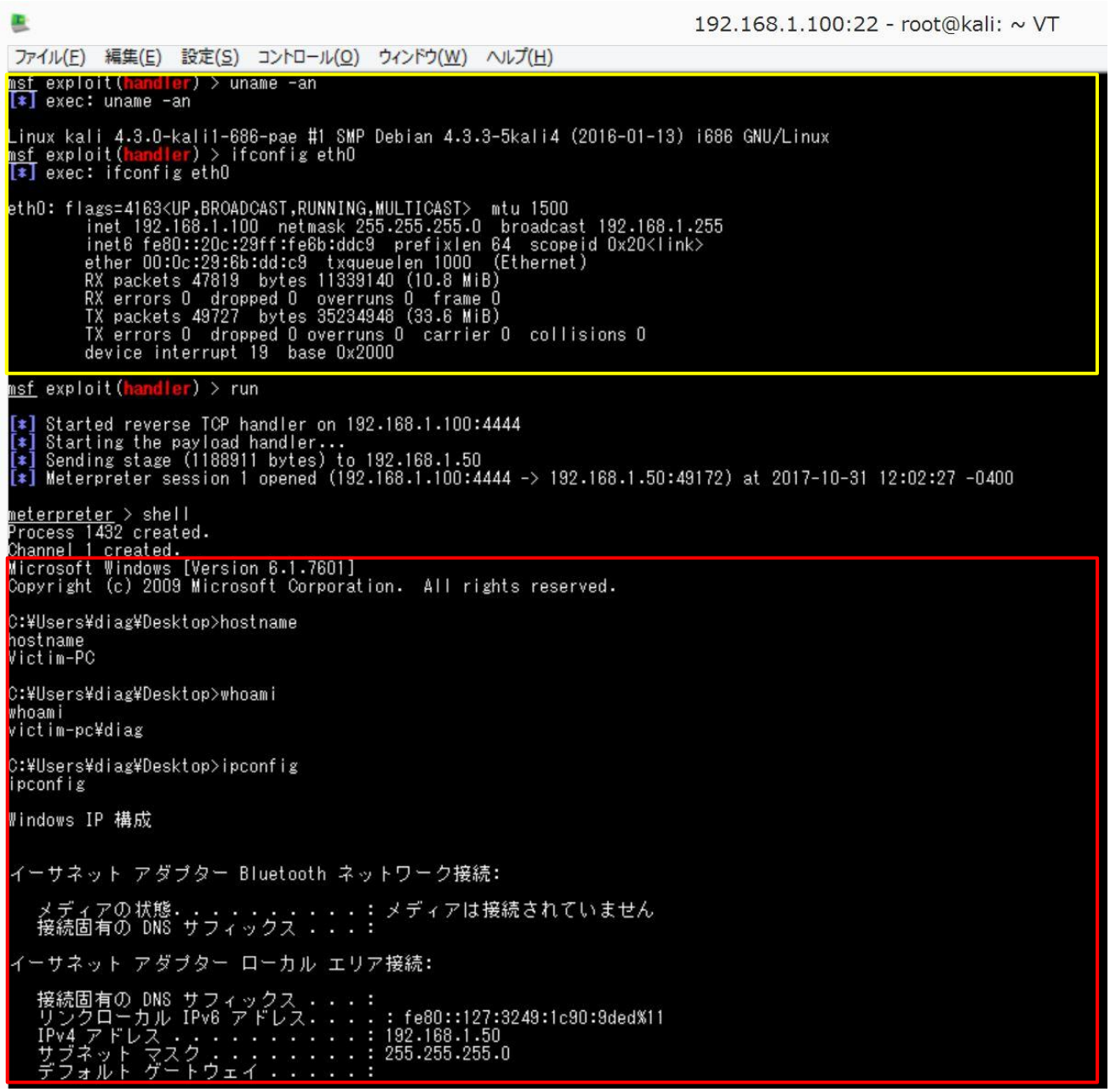


【検証結果】

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。



なお、上記対策案の数式エディター 3.0 を無効した場合、および、EMET の ASLR をシステム全体のレベルで「Always On」にした場合には、任意のコマンドが実行できず攻撃が成立しないことが確認できました。

【更新履歴】 2017 年 11 月 27 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/