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 Internet Explorer 9 から 11 ほか、他製品で使用されている JScript 5.8 および VBScript 5.7 または 5.8 エンジンにおける任意のコードを実行される脆弱性（CVE-2016-0189）(MS16-051 および MS16-053)に関する調査レポート

【概要】

Internet Explorer 9 から 11 およびその他製品で使用されている、 Microsoft JScript 5.8 および VBScript 5.7 または 5.8 エンジンにおいて、任意のコードを実行、またはサービス拒否状態にされる脆弱性(CVE-2016-0189) (MS16-051 および MS16-053)の攻撃コードが発見されました。この攻撃コードは 2016 年 6 月頃に発見されたものですが、同脆弱性は 2016 年にエクスプロイトキット（=Magnitude, Neutrino, RIG, Sundown Exploit Kit）で最も悪用された脆弱性であるとの Recorded Future による報告があり、改めての注意喚起の意味を込めて、本レポートを作成いたしました。なお、この脆弱性は、使用する配列をロックしていないことにより、配列を使用中に同配列のプロパティ等が変更可能であることが原因で生じるものです。

本脆弱性を利用した攻撃が成立した場合、攻撃者により細工された Web サイトを介して、任意のコードを実行される、またはサービス拒否状態にされる可能性があります。

本レポート作成時点（2016 年 12 月 15 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（2016 年 5 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から、今回、この脆弱性（CVE-2016-0189）(MS16-051 および MS16-053)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 Internet Explorer 9
  - 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
- Microsoft Internet Explorer 10
  - Windows Server 2012
- Microsoft Internet Explorer 11
  - 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 8.1 for 32-bit Systems
  - Windows 8.1 for x64-based Systems
  - Windows Server 2012 R2
  - Windows RT 8.1
  - Windows 10 for 32-bit Systems
  - Windows 10 for x64-based Systems
  - Windows 10 Version 1511 for 32-bit Systems
  - Windows 10 Version 1511 for x64-based Systems
- VBScript 5.7
  - Windows Vista Service Pack 2
  - Windows Vista x64 Edition Service Pack 2
  - Windows Server 2008 for x32-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 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)
- JScript 5.8 および VBScript 5.8
  - Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core インストール)

【対策案】

Microsoft 社より、この脆弱性を修正する更新プログラム（MS16-053 および MS16-051）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。

更新プログラムを適用しない場合の回避策として、下記「VBScript.dll および JScript.dll へのアクセスの制限」を行う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、VBScript または JScript を使用する Web サイトが正常に機能しない場合があると報告されています。

- 32 ビットコンピュータの場合、管理コマンドプロンプトから下記コマンドを入力します。

```
takeown /f %windir%¥system32¥vbscript.dll
cacls %windir%¥system32¥vbscript.dll /E /P everyone:N
cacls %windir%¥system32¥jscript.dll /E /P everyone:N
```

- 64 ビットコンピュータの場合、管理コマンドプロンプトから下記コマンドを入力します。

```
takeown /f %windir%¥syswow64¥vbscript.dll
cacls %windir%¥syswow64¥vbscript.dll /E /P everyone:N
cacls %windir%¥syswow64¥jscript.dll /E /P everyone:N
```

【バージョン確認方法】

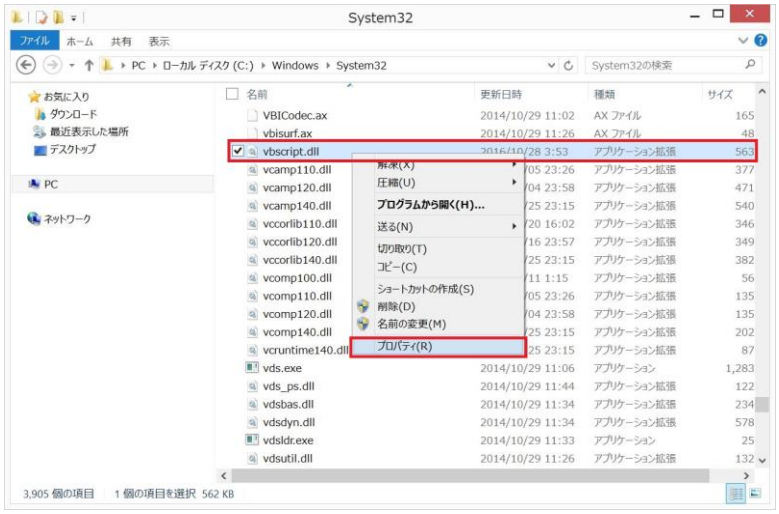
以下の手順でシステムにインストールされている JScript または VBScript エンジンのバージョンを確認することができます。

1. エクスプローラーを起動します。
2. %systemroot%¥system32 ディレクトリに移動します。

VBScript の場合

[vbscript.dll]を右クリックして [プロパティ]を選択し、次に [詳細]タブをクリックします。

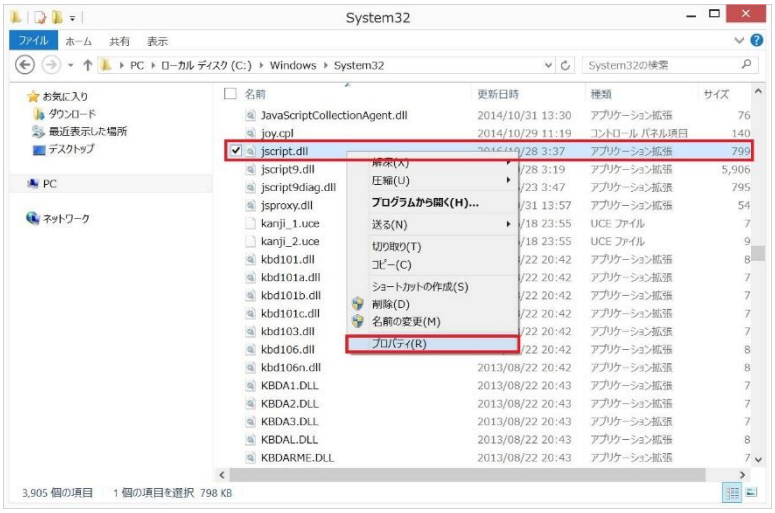
ファイルバージョンが 5.8 で始まる場合（例: 5.8.9600.18525)、VBScript 5.8 がコンピューターにインストールされています。



JScript の場合

[jscript.dll]を右クリックして [プロパティ]を選択し、次に [詳細]タブをクリックします。

ファイルバージョンが 5.8 で始まる場合（例: 5.8.9600.18525)、JScript 5.8 がコンピューターにインストールされています。



【参考サイト】

CVE-2016-0189

Internet Explorer 9 から 11 などの製品で使用される Microsoft JScript および VBScript エンジンにおける任意のコードを実行される脆弱性

マイクロソフト セキュリティ情報:MS16-051

マイクロソフト セキュリティ情報:MS16-053

New Kit, Same Player: Top 10 Vulnerabilities Used by Exploit Kits in 2016

【検証概要】

ターゲットシステムを攻撃者が用意したサイトにアクセスさせることで、JScript および VBScript エンジンの脆弱性を利用して任意のコードを実行させます。

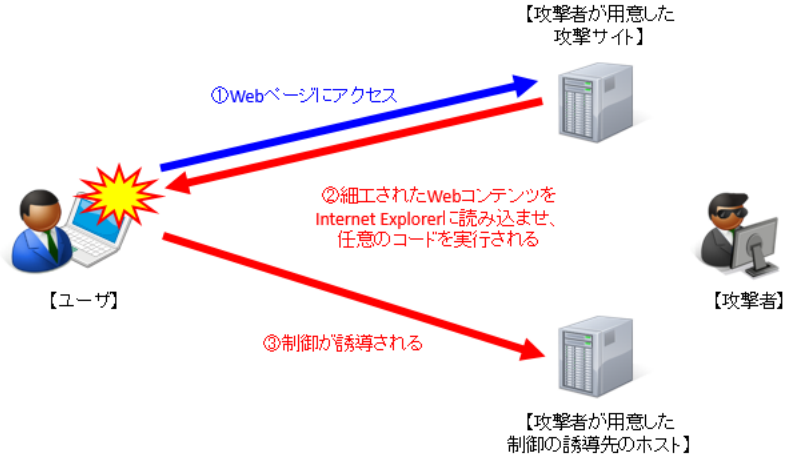
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバー、ポートにコネクションを確立させるよう誘導し、システム制御を奪取するものです。これにより、リモートからターゲットシステムが操作可能となります。

*誘導先のシステムは Linux です。

【検証ターゲットシステム】

Windows 10 日本語版 + Internet Explorer 11

【検証イメージ】

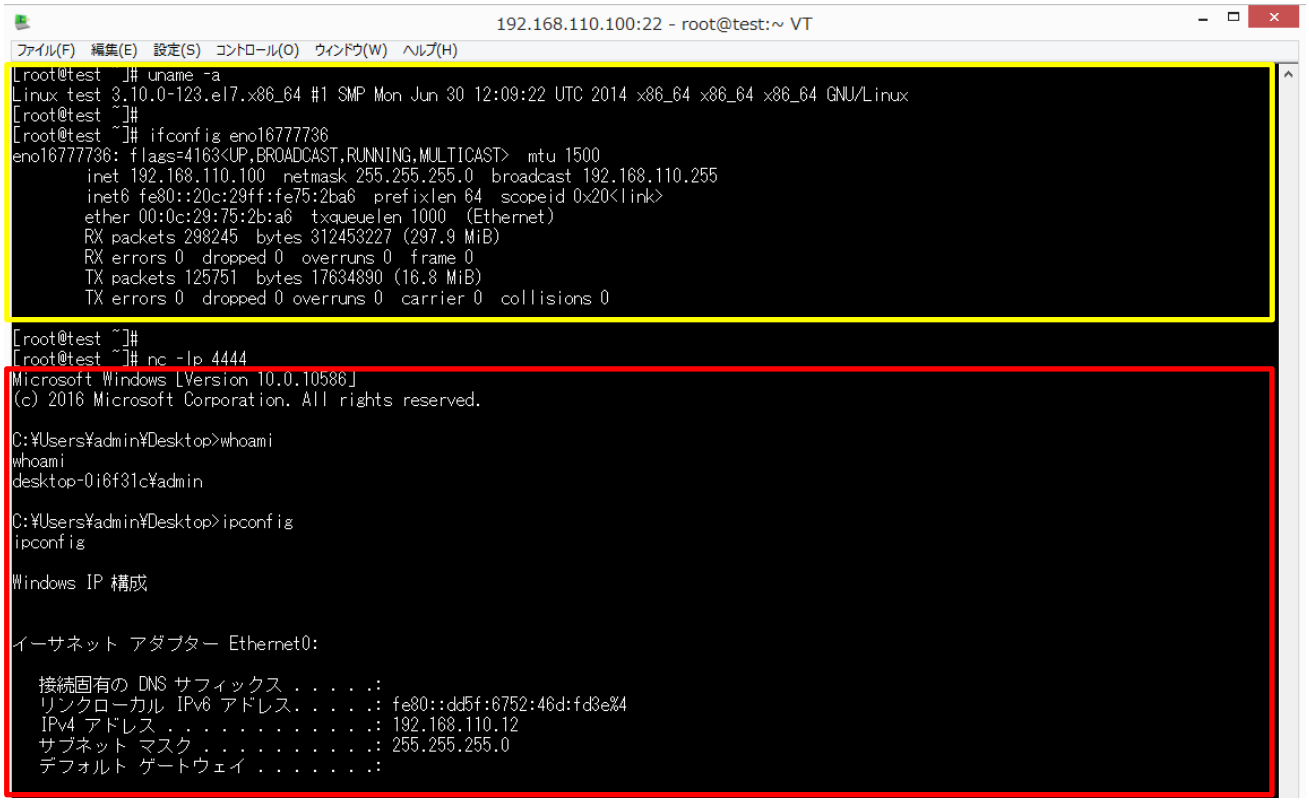


【検証結果】

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(Windows 10)において、ホスト名、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】

2016 年 12 月 22 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/