Microsoft Windows 製品の SMBv1 サーバーの脆弱性により、リモートから任意のコードが実行可能な脆弱性（MS17-010）に関する調査レポート

【概要】

Microsoft Windows 製品の SMBv1（サーバー メッセージ ブロック 1.0）サーバーに、リモートより任意のコードが実行可能な脆弱性（MS17-010）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、SMBv1 サーバーが特定のリクエストを処理する際の不具合に起因する脆弱性で、この脆弱性を利用した攻撃が成立した場合、リモートから Windows の SYSTEM 権限で任意のコードを実行される危険性があります。
また、本脆弱性は、「Shadow Brokers」と名乗るグループによって公開された、米国家安全保障局（NSA）が使用したとする攻撃コードの中の一つである「EternalBlue」が悪用する脆弱性で、本脆弱性が存在するターゲットに対して同コードを使用し、ターゲットを「DOUBLEPULSAR」と呼ばれるリモートから任意のコードが実行可能なバックドアに感染させる攻撃を観測したとの報告もあります。

本レポート作成（2017 年 5 月 8 日）時点において、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 3 月 15 日付）。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（MS17-010）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】

- Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 2
- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows 8.1 for 32-bit Systems
- Windows 8.1 for x64-based Systems
- 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
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1607 for x64-based Systems
- Windows Server 2008 for 32-bit 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
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core インストール)
- Windows Server 2008 for Itanium-based Systems Service Pack 2
- Windows Server 2008 R2 for x64-based Systems Service Pack 1

- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core インストール)
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
- Windows Server 2012
- Windows Server 2012 (Server Core インストール)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core インストール)
- Windows Server 2016 for x64-based Systems
- Windows Server 2016 for x64-based Systems (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、SMB サーバーにて SMBv1 を無効にする方法が提案されています。なお、SMBv1 を無効にすることにより、SMBv1 以外の SMB バージョンをサポートしていない機器と、ファイル共有等の SMB を使用した通信ができなくなる可能性があるため、同回避策を使用する場合には代替の通信方法を検討する必要があります。

SMB サーバーにて SMBv1 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 enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server

- 「Windows Vista、Windows 7、Windows Server 2008 および Windows Server 2008 R2」を実行している場合

1. [Windows PowerShell※] を管理者権限で実行し、以下のコマンドレットを実行します。
   ※Windows PowerShell 2.0 またはそれ以降のバージョンの PowerShell

```
Set-ItemProperty -Path "HKLM:¥SYSTEM¥CurrentControlSet¥Services¥LanmanServer¥Parameters"
SMB1 -Type DWORD -Value 0 -Force
```

2. コンピューターを再起動します。

- 「Windows 8 および Windows Server 2012」を実行している場合

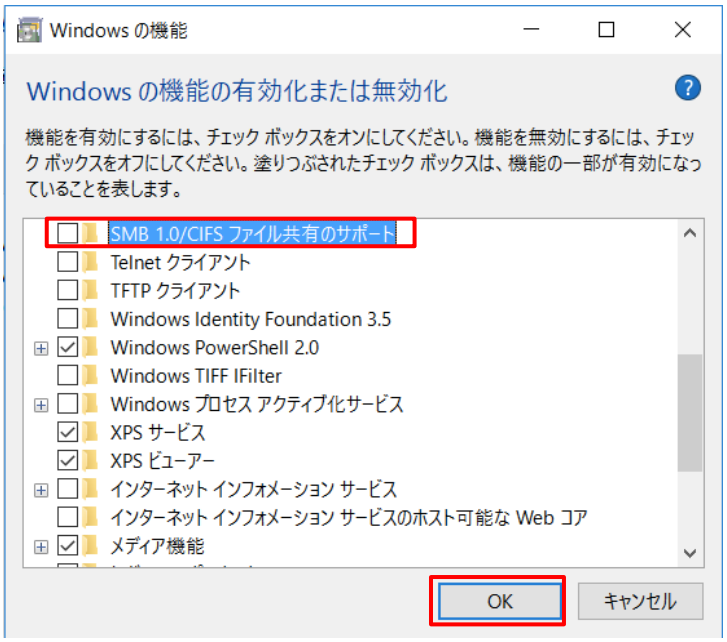
1. [Windows PowerShell] を管理者権限で実行し、以下のコマンドレットを実行します。

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

- 「Windows 8.1」以降のクライアントオペレーティングシステムを実行している場合

1. [コントロールパネル] を開き、[プログラムと機能] を選択。右ペインの[Windows の機能の有効化または無効化] をクリックします。

2. Windows の機能にて [SMB1.0/CIFS ファイル共有のサポート] のチェックボックスをオフにし、[OK] ボタンをクリックします。

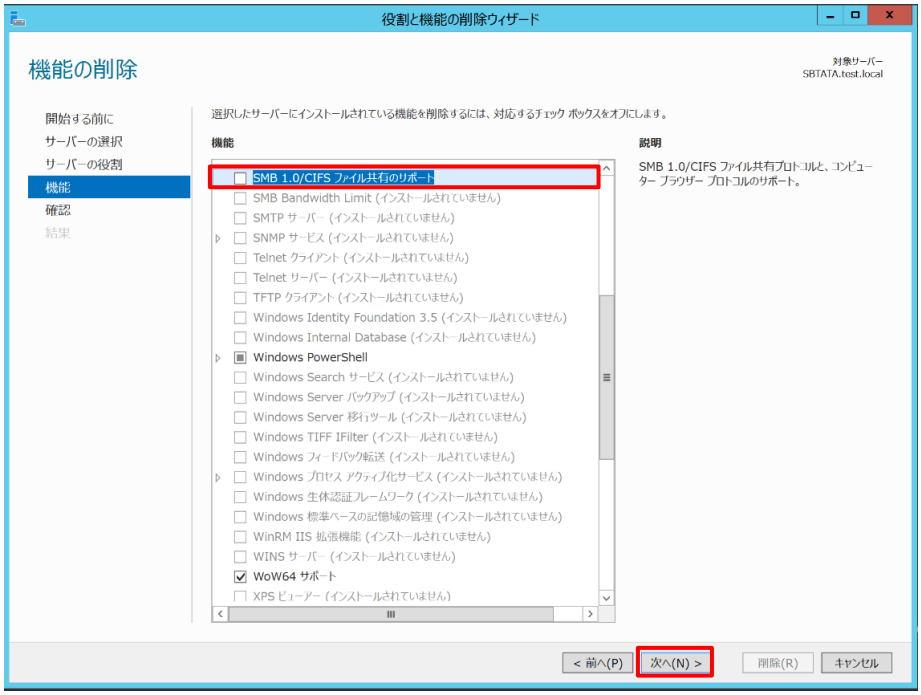


3. コンピューターを再起動します。

- 「Windows Server 2012 R2」以降のサーバーオペレーティングシステムを実行している場合

1. ［サーバーマネージャー］を開き、［管理］メニューを選択。［役割と機能の削除］をクリックします。

2. 役割と機能の削除ウィザードにて［SMB1.0/CIFS ファイル共有のサポート］のチェックボックスをオフにし、［次へ］ボタンをクリック。削除オプションの確認にて[削除]ボタンをクリックします。



3. コンピューターを再起動します。

【参考サイト】

- マイクロソフト セキュリティ情報 MS17-010 - 緊急
- Protecting customers and evaluating risk
- DoublePulsar Global Implants: On the rise?
- How to enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server

【検証概要】

攻撃者は、SMBv1 サーバーとして動作するターゲットシステムへ細工したリクエストを送信することにより、ターゲットシステムの脆弱性を利用して任意のコードを実行させます。

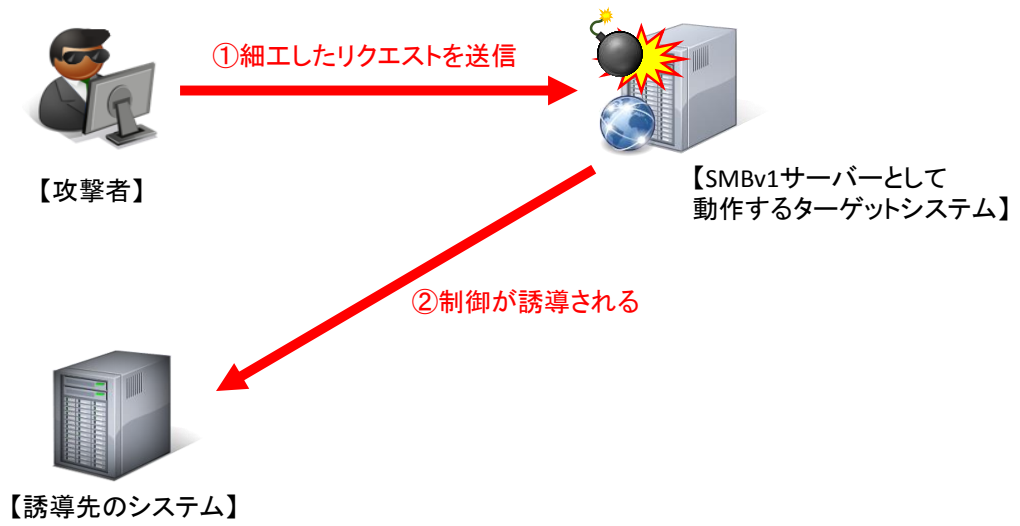
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバー、ポートへコネクションを確立させるよう誘導し、システム制御を奪取するものです。これにより、リモートから Windows の SYSTEM 権限でターゲットシステムが操作可能となります。

*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 Professional SP1 日本語版

【検証イメージ】

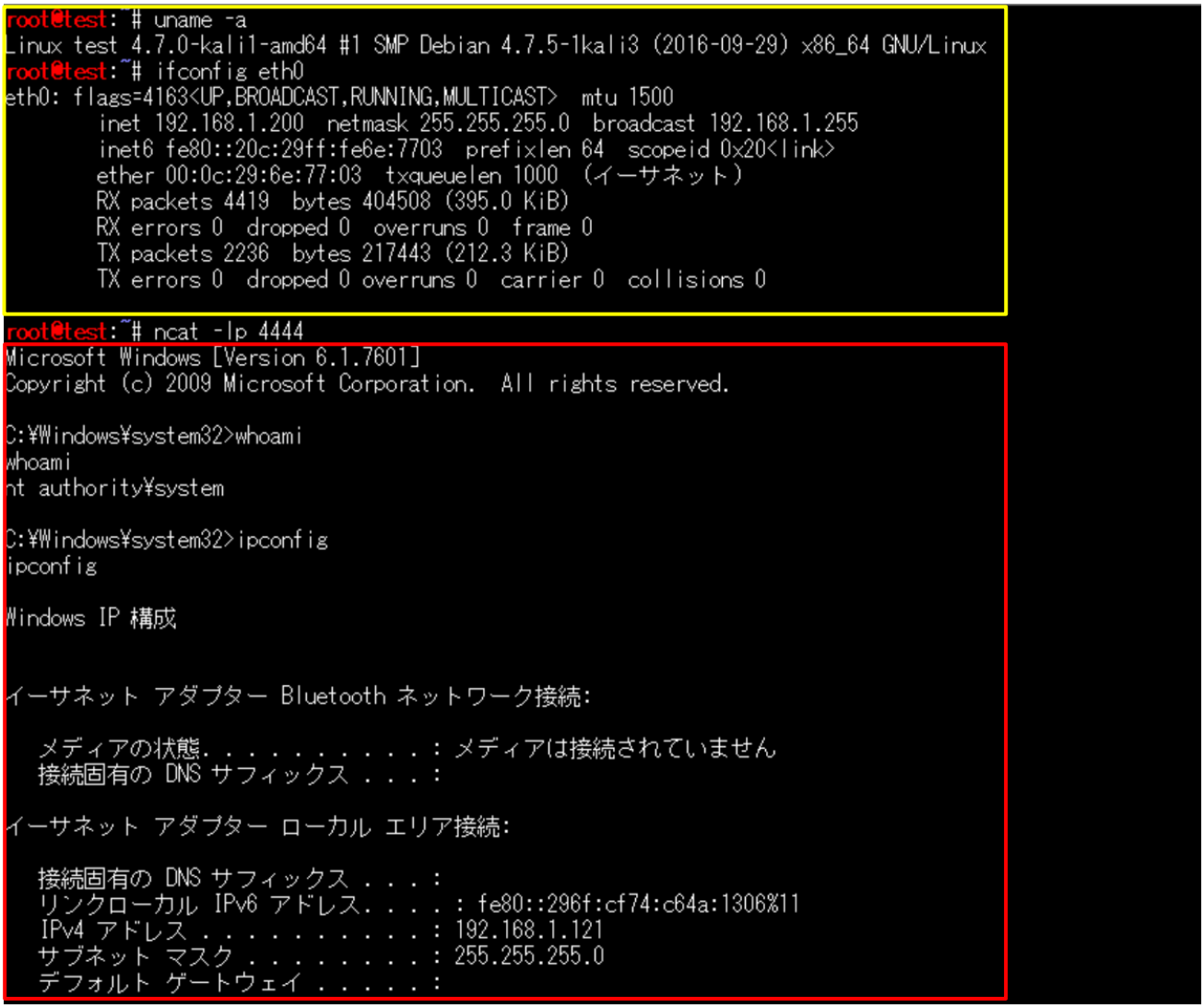


【検証結果】

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。



【更新履歴】 2017 年 5 月 8 日 ： 初版公開

【本レポートに関するお問い合わせは下記まで】

『報道関係者様からのお問い合わせ』 ソフトバンク・テクノロジー株式会社　管理本部　経営企画部　齊藤、安部、菅

TEL：03-6892-3063　メールアドレス：sbt-pr@tech.softbank.co.jp

『お客様からのお問い合わせ』下記フォームよりお問い合わせください。

https://info.softbanktech.jp/public/application/add/508