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 Windows 製品の Windows Shell 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-2017-8464）に関する調査レポート

【概要】

Microsoft Windows 製品の Windows Shell に、リモートより任意のコードが実行可能な脆弱性（CVE-2017-8464）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、Windows エクスプローラーなどでショートカットのアイコンを表示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、ショートカットのアイコンを表示する操作を行っ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。

本レポート作成（2017 年 8 月 15 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 6 月 14 日付(日本時間)）。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-2017-8464）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 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 10 Version 1703 for 32-bit Systems
- Windows 10 Version 1703 for x64-based Systems
- 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 Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for Itanium-Based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- 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 Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Server 2016 (Server Core installation)

【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。

【参考サイト】

- CVE - CVE-2017-8464
- CVE-2017-8464 | LNK のリモートでコードが実行される脆弱性
- マイクロソフト セキュリティ アドバイザリ 4025685

【検証概要】

検証は下記の 2 パターンについて実施しました。

- 検証パターン 1

攻撃者は、細工した LNK ファイル(ショートカットファイル)および同ファイルに関連付けられた悪意のあるバイナリを USB メモリに保存。ターゲットシステムで同 USB メモリを接続し、Windows エクスプローラーで開くことにより、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。

- 検証パターン 2

攻撃者は、細工した LNK ファイル(ショートカットファイル)および同ファイルに関連付けられた悪意のあるバイナリをファイルサーバー上のネットワークドライブに保存。ターゲットシステムで同ファイルが存在するフォルダに対して、ネットワークドライブの割り当てを行い、Windows エクスプローラーで同ドライブを開くことにより、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、検証パターン 1 および 2 ともに、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で USB メモリまたはネットワークドライブを Windows エクスプローラーで開いたユーザーの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。

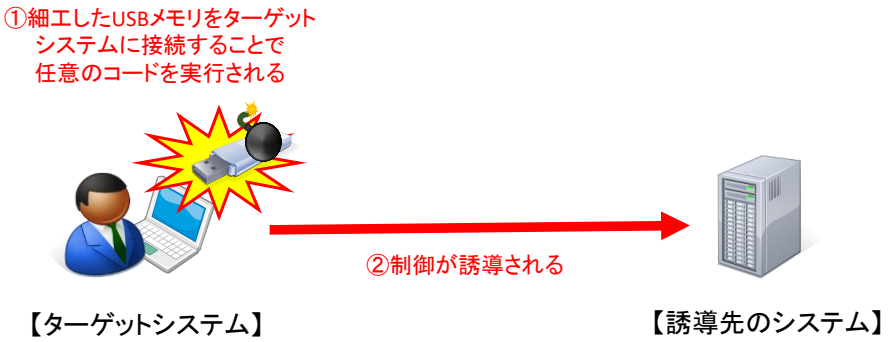
【検証ターゲットシステム】

検証パターン 1 および 2 ともに以下のターゲットシステムを使用しました。

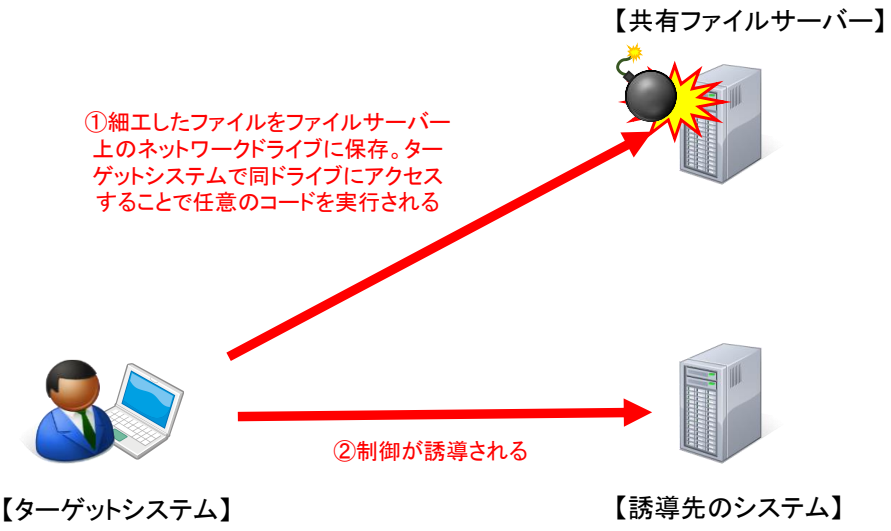
- Windows 7 Professional SP1　日本語版

【検証イメージ】

- 検証パターン 1



- 検証パターン 2



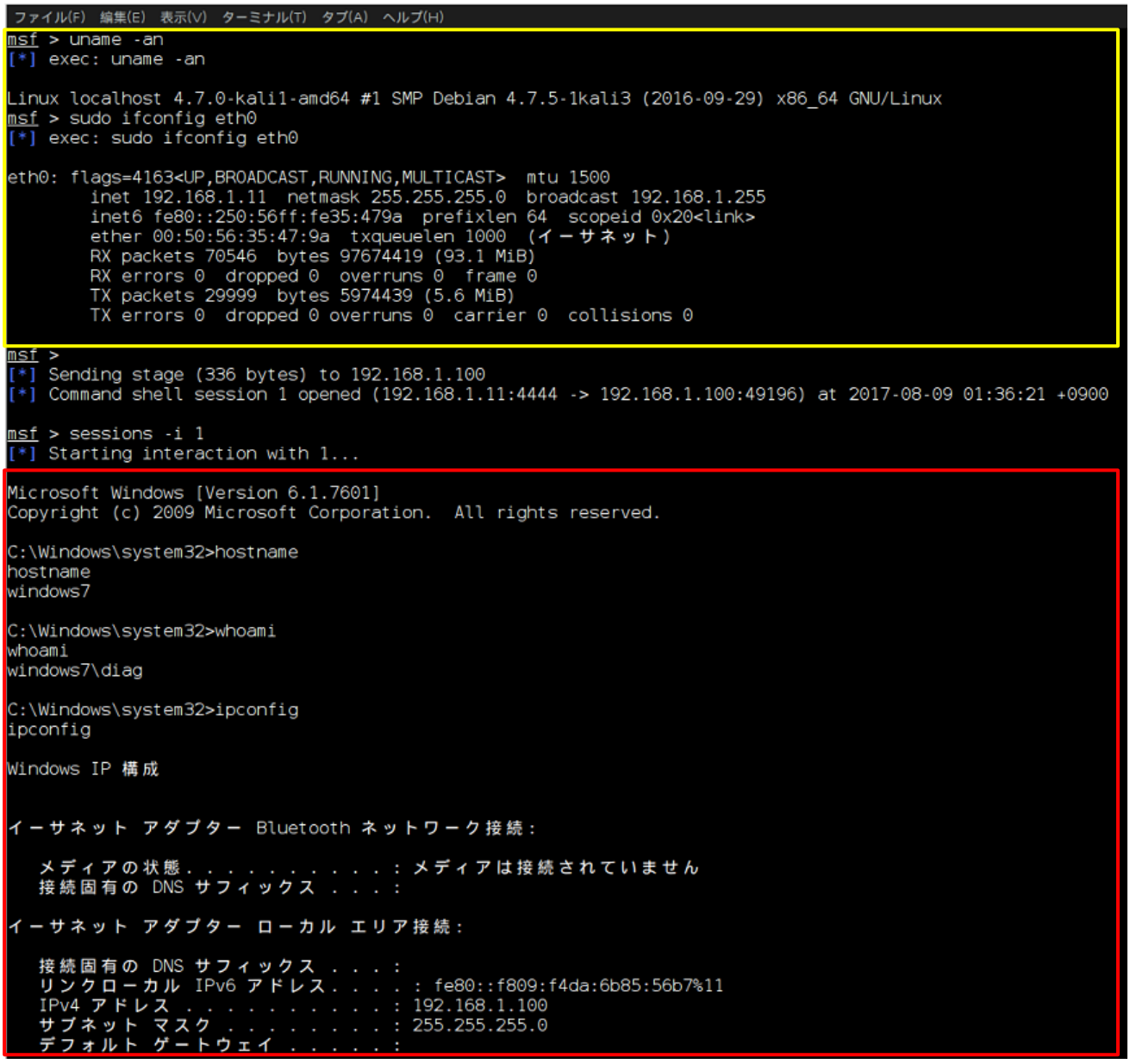
【検証結果】

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。

※　検証パターン 1 および 2 ともに同様の結果が得られました。



【更新履歴】

2017 年 8 月 15 日 ： 初版公開

2017 年 8 月 22 日 ： 検証について共有ファイルサーバーを利用して任意のコードを実行させる検証パターンを追記

【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

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/