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

Windows の DLL ファイル処理の脆弱性により、リモートから任意のコードが実行可能な脆弱性（CVE-2015-0096）(MS15-020)に関する調査レポート

【概要】

Microsoft Windows で DLL ファイルを処理する際に、リモートから任意のコードを実行可能な脆弱性（CVE-2015-0096）が発見されました。この脆弱性は、DLL ファイルを処理する際に問題があり、ユーザに細工された Web サイトやファイル、DLL ファイルが含まれる作業ディレクトリ内のファイルを開かせることにより、リモートより任意のコードを実行することが可能です。

この脆弱性を利用した攻撃が成立した場合、ログオンしているユーザと同じ権限を奪取される危険性があります。

本レポート作成（2015 年 3 月 19 日）時点において、既に Microsoft 社より脆弱性の修正プログラムがリリースされております（2015 年 3 月 10 日）。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-2015-0096）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 Server 2003 Service Pack 2
- Windows Server 2003 x64 Edition Service Pack 2
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2（Server Core インストールを含む）
- Windows Server 2008 for x64-based Systems Service Pack 2（Server Core インストールを含む）
- Windows Server 2008 for Itanium-based Systems Service Pack 2
- 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（Server Core インストールを含む）
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
- Windows 8 for 32-bit Systems
- Windows 8 for x64-based Systems
- Windows 8.1 for 32-bit Systems
- Windows 8.1 for x64-based Systems
- Windows Server 2012（Server Core インストールを含む）

- Windows Server 2012 R2（Server Core インストールを含む）
- Windows RT
- Windows RT 8.1

【対策案】

Microsoft 社より、この脆弱性を修正するプログラム（MS15-020）がリリースされています。
当該脆弱性が修正された修正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-2015-0096

- Microsoft Windows の脆弱性により、リモートでコードが実行される（3041836）

- 複数の Microsoft Windows 製品における権限昇格の脆弱性

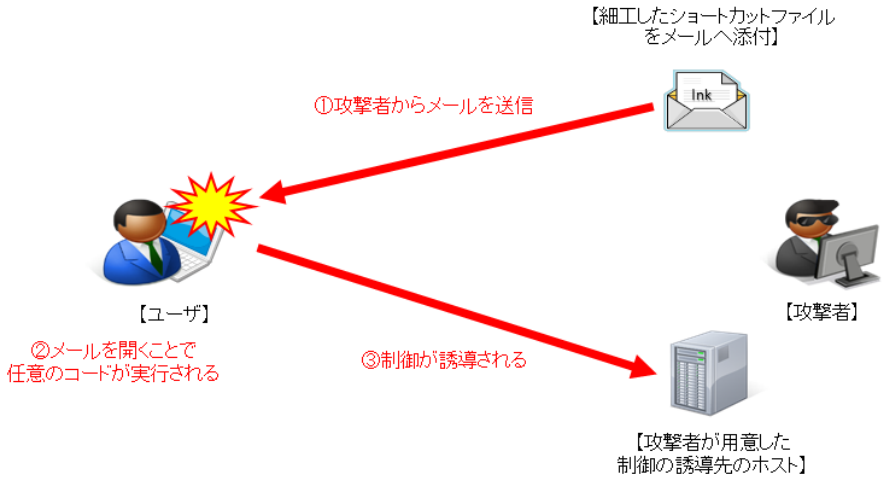
【検証概要】

ターゲットシステムのユーザに対して、細工したショートカットファイルを添付したメールを送信します。ユーザがそのメールを開くことにより、ターゲットシステムは悪意のあるユーザが用意したホストへと制御が誘導されます。
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、システムの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 CentOS です。

【検証ターゲットシステム】

Windows Server 2003 SP2
Windows Server 2008 SP2

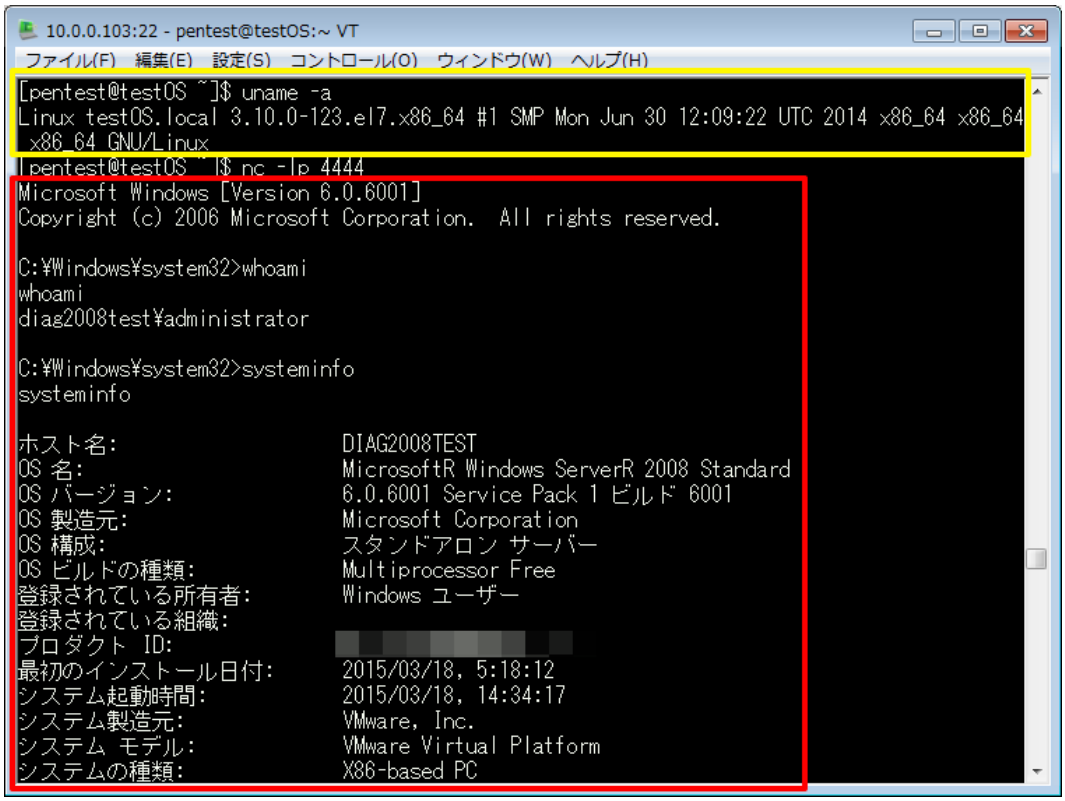
【検証イメージ】



【検証結果】

下図は、誘導先のコンピュータ（CentOS）の画面です。黄線で囲まれている部分は、誘導先のコンピュータの情報です。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 Server 2008）において、ホスト名、ユーザの情報、システム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。



SoftBank Technology

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/