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

Windows のカーネルモードドライバの脆弱性により、権限昇格が行える脆弱性（CVE-2015-1701）(MS15-051)に関する調査レポート

【概要】

Microsoft Windows のカーネルモードドライバ（Win32k.sys）に、ローカルから権限昇格を行える脆弱性（CVE-2015-1701）が発見されました。

この脆弱性は、Win32k.sys がメモリ内のオブジェクトを正しく処理しないことにより発生します。これにより、システム上で権限昇格を行うことができ、その後カーネルモードで任意のコードの実行が可能となります。

攻撃者がこの脆弱性を利用するためには、システムへの有効なログオン情報が必要になります。

攻撃者が何らかの方法でシステムの一般ユーザーでのアクセス権を獲得した場合、この脆弱性を利用することでSYSTEM 権限を奪取されます。その結果、SYSTEM 権限でシステムを操作し、重要情報の改ざん、窃取されてしまうといった危険性があります

本レポート作成（2015 年 5 月 25 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 5 月 13 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-2015-1701）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（MS15-051）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-2015-1701

- Windows カーネルモード ドライバーの脆弱性により、特権が昇格される (3057191)

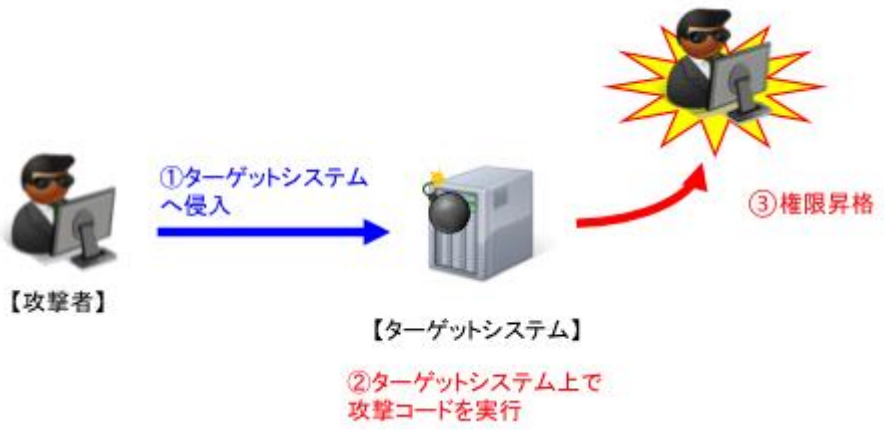
【検証概要】

攻撃者は、一般ユーザー権限でターゲットシステムにログオンした後、細工したファイルを実行します。これにより、ログオン時のユーザー権限から SYSTEM 権限へ昇格するというものです。

【検証ターゲットシステム】

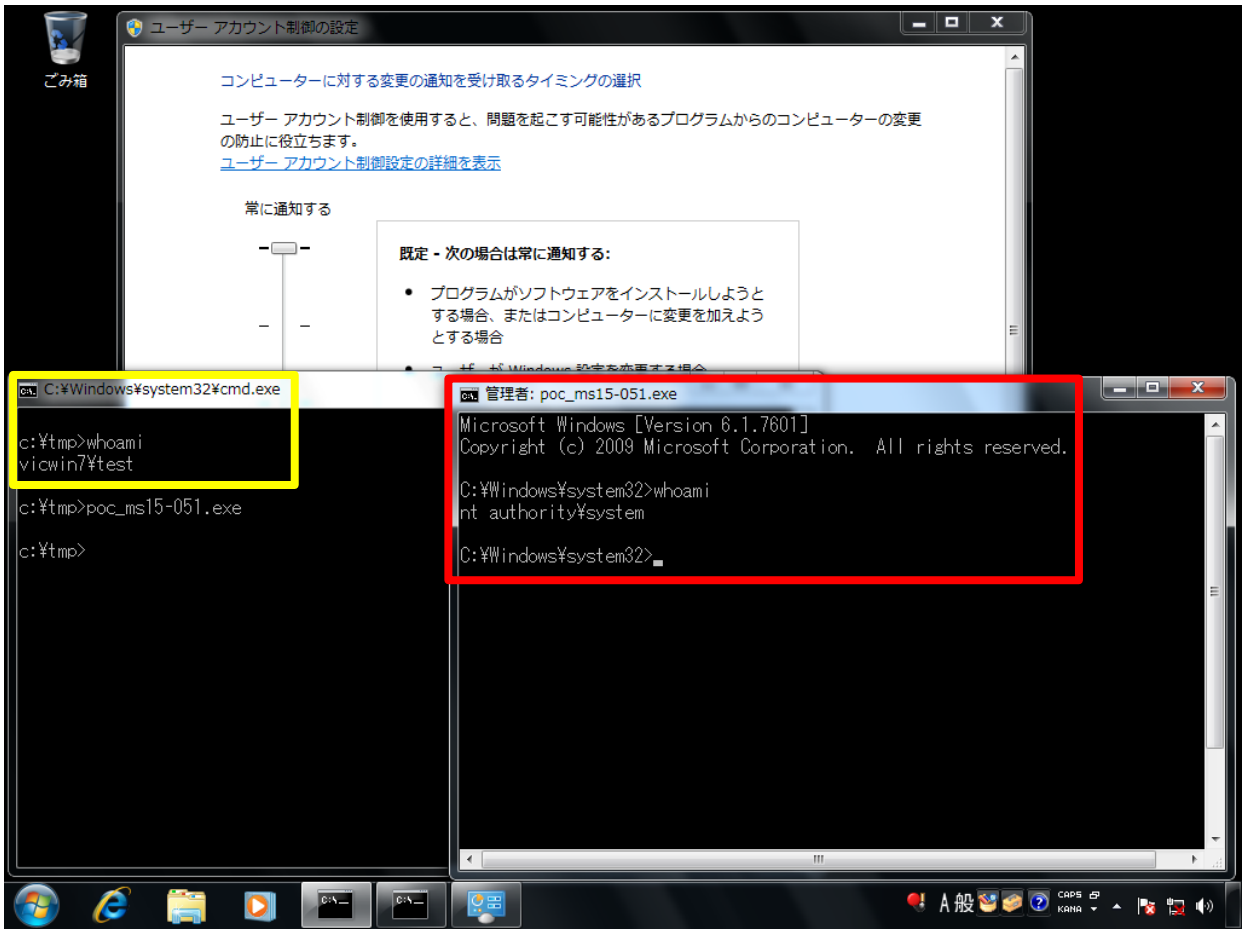
Windows 7 SP 1

【検証イメージ】



【検証結果】

下図は、ターゲットシステム（Windows 7）の画面です。黄枠の箇所は、ログオン直後のユーザー情報（test）を表示しています。一方で赤枠の箇所は、細工されたプログラムを実行した直後のもので、SYSTEM 権限でコマンドプロンプトが動作していることを確認できます。細工されたプログラムを実行する際、UAC（ユーザーアカウント制御）による制御が有効であっても、制御は回避されてしまいます。



【更新履歴】

2015 年 5 月 25 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/