Windows セカンダリログオンの脆弱性により、権限昇格が行える脆弱性(CVE-2016-0099)(MS16-032)に関する調査レポート

【概要】

Microsoft Windows セカンダリログオンに、ローカルから権限昇格を行える脆弱性（CVE-2016-0099）についての PowerShell スクリプトを用いた新しい攻撃方法が発見されました。
この脆弱性は、セカンダリログオンサービスが要求ハンドラー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管理者権限も同時に掌握されます。その結果、管理者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（2016 年 4 月 26 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（2016 年 3 月 9 日付）。
なお PowerShell スクリプトは、デフォルトで実行ポリシーによりスクリプトの実行が禁止されており、スクリプトを実行するためには管理者 PowerShell より実行ポリシーを変更する必要があります。しかしながら、一般ユーザー権限でこの制限を回避する方法があります。このため、脆弱性による攻撃を容易に行うことが可能であり、かつ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-2016-0099）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 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 8.1 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 8.1
- Windows 10 for 32-bit Systems

- Windows 10 x64-based Systems
- Windows 10 Version 1511 for 32-bit Systems
- Windows 10 Version 1511 for x64-based Systems

【対策案】

Microsoft 社より、この脆弱性を修正するプログラム（MS16-032）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。
なお、本レポート作成時点では、問題を緩和する要素および、回避策については Microsoft 社より提示されていません。

【参考サイト】

- CVE-2016-0099
- 特権の昇格に対処するセカンダリ ログオン用のセキュリティ更新プログラム (3143141)

【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 PowerShell スクリプトを実行します。これにより、ログオン時のユーザー権限よりも上位の権限に昇格するというものです。

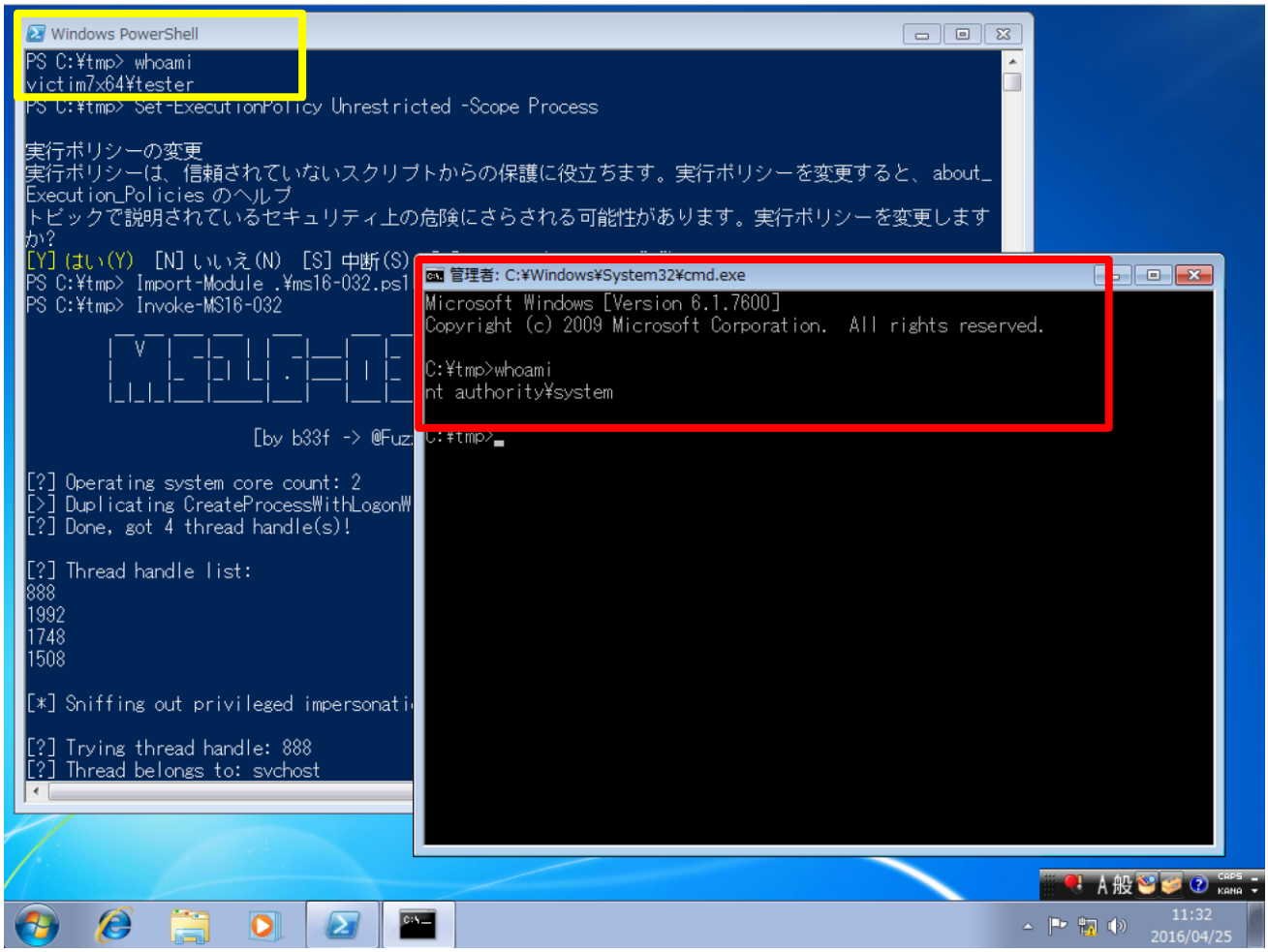
【検証ターゲットシステム】

Windows 7 Professional SP1
Windows Server 2012 R2

【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、PowerShell 上でログオン直後のユーザー権限（tester）を表示した結果を表しています。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。



【更新履歴】

2016 年 4 月 26 日 ： 初版公開