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

HTTP.sys ファイルの処理の脆弱性により、リモートから任意のコードを実行可能な脆弱性（CVE-2015-1635）(MS15-034)に関する調査レポート

【概要】

Microsoft Windows のコンポーネントである HTTP.sys が HTTP リクエストを処理する際に、リモートから任意のコードを実行可能な脆弱性（CVE-2015-1635）が発見されました。この脆弱性は、細工された HTTP リクエストをターゲット上の IIS に送信することにより、システム権限で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、リモートからシステム権限を奪取される危険性があります。なお、本レポート作成（2015 年 4 月 16 日）時点において、システムにおけるサービス拒否を発生させる攻撃方法が公開されています。現時点ではシステムをダウンさせることにのみ成功しておりますが、今後、任意のコードの実行を実現する攻撃コードがリリースされる可能性がありますので、**可能な限り早急に対策を講じていただくことを強く推奨**いたします。

本レポート作成（2015 年 4 月 16 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 4 月 15 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から、今回、この脆弱性（CVE-2015-1635）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 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）

【対策案】

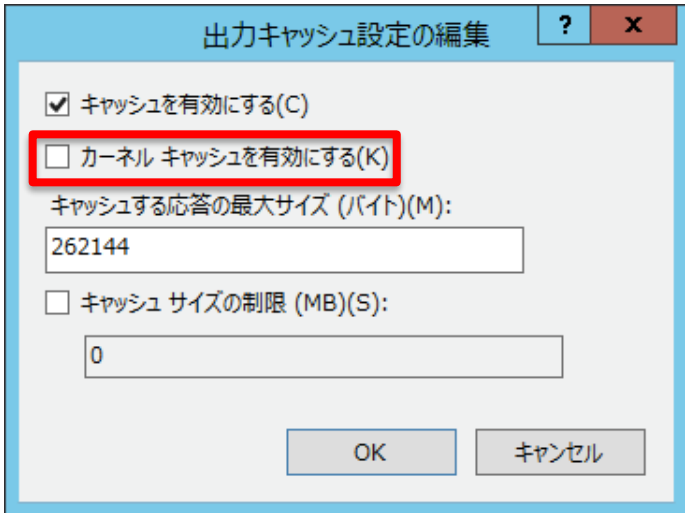
Microsoft 社より、この脆弱性を修正するプログラム（MS15-034）がリリースされています。

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。

ただちに修正プログラムを適用することが困難な場合、Microsoft 社より提供されている次の回避策の実施を推奨い

たします。
IIS の[出力キャッシュ]の設定より、[カーネルキャッシュを有効にする]のチェックを外すことにより、この脆弱性利用する攻撃を回避することが可能です。設定後、IIS を再起動する必要はありません。
ただし、この設定を行うことにより、IIS のパフォーマンスが低下する可能性があります。

参考:カーネル キャッシュを有効にする (IIS 7)
※参照先ページはカーネルキャッシュを有効にする設定が紹介されていますが、この脆弱性の回避策は「無効」にしていただくことです。



【参考サイト】
- CVE-2015-1635

- HTTP.sys の脆弱性により、リモートでコードが実行される (3042553)

【検証概要】
IIS が動作するターゲットシステムに対して細工した HTTP リクエストを送信することにより、ターゲットシステムで BSOD (Blue Screen of Death)を発生させ、システムをダウンさせます。

【検証ターゲットシステム】
Windows Server 2008 R2 SP1 (IIS7.5)
Windows Server 2012 (IIS8.0)
Windows Server 2012 R2 (IIS8.5)

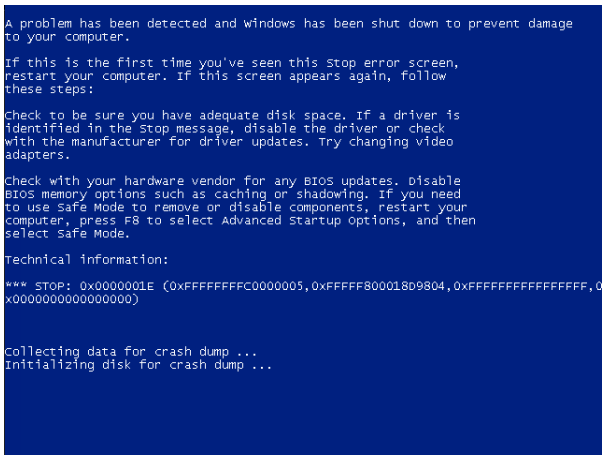
【検証イメージ】

【検証結果】

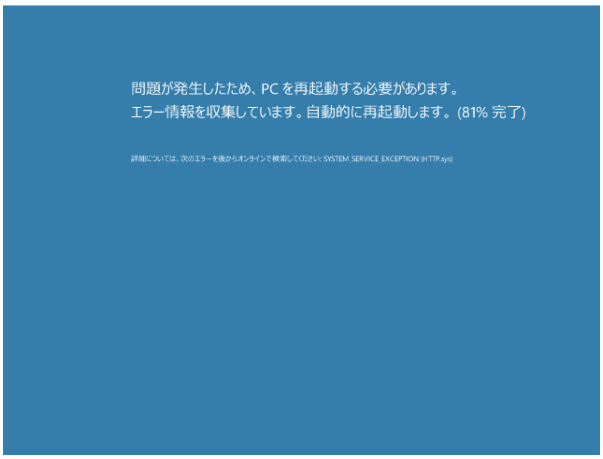
下図は、ターゲットシステム（Windows Server 2008R2 および Windows Server 2012）の画面です。図のように、細工された HTTP リクエストを受信したターゲットシステムでは BSOD が発生し、ダウンします。

また https 通信においても、この脆弱性が発現することが確認できております。

（Windows Server 2008R2 の場合）



（Windows Server 2012 の場合）



【更新履歴】

2015 年 4 月 16 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/