NTT DATA
NTTデータ 先端技術株式会社

HTTP.sys の脆弱性により、リモートでコードが実行される(MS15-034)(CVE-2015-1635)に関する検証レポート

2015/04/17
NTT データ先端技術株式会社
山野 泰章

【概要】

Windows の Microsoft HTTP プロトコルスタックをつかさどるドライバーである HTTP.sys に、リモートより任意のコードが実行される脆弱性(CVE-2015-1635)が発見されました。HTTP.sys において HTTP リクエストを解析する処理に不備があり、細工された HTTP リクエストを受け取るとオーバーフローが発生します。

攻撃者は、この脆弱性を利用することにより HTTP を提供する Microsoft IIS 等の HTTP.sys を使ってサービスを提供する Windows 7 以降の Windows OS 上でシステム停止や任意のコードを実行する可能性があります。

今回、この脆弱性 (MS15-034) (CVE-2015-1635) の再現性について検証を行いました。

【影響を受けるとされているシステム】

影響を受ける可能性が報告されているシステムは次のとおりです。

- 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
- 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
- Windows Server 2012 R2
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core インストール)
- Windows Server 2012 (Server Core インストール)
- Windows Server 2012 R2 (Server Core インストール)

【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。
当該脆弱性に対する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】

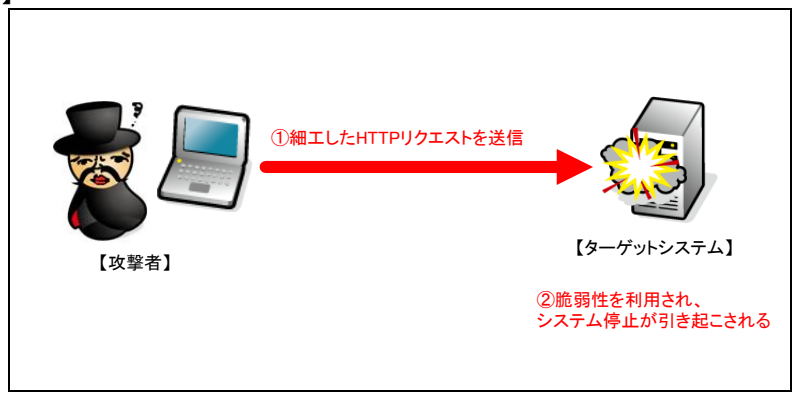
CVE-2015-1635
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1635

HTTP.sys の脆弱性により、リモートでコードが実行される (3042553)
https://technet.microsoft.com/library/security/MS15-034

Microsoft 製品の脆弱性対策について(2015 年 4 月)
http://www.ipa.go.jp/security/ciadr/vul/20150415-ms.html

Copyright © 2015. NTT DATA INTELLILINK CORPORATION All right reserved.

【検証イメージ】

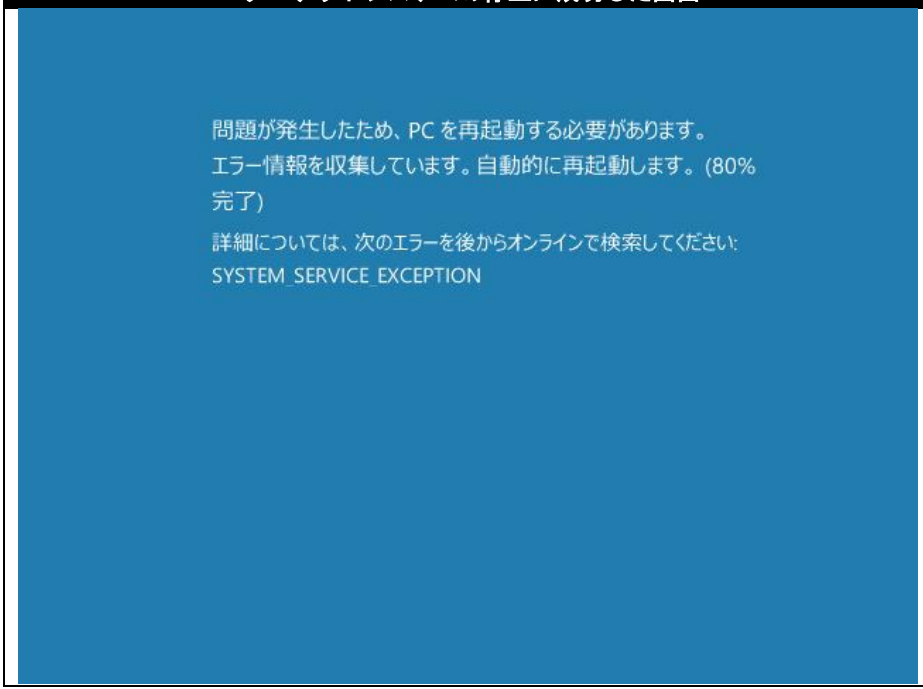


【検証ターゲットシステム】
Windows Server 2012 R2 上の IIS8.5

【検証概要】
ターゲットシステムで Microsoft IIS が稼動しているポートに対して、細工した HTTP リクエストを送信し、ターゲットシステムを停止させるものです。攻撃コードを改変することにより、リモートからターゲットシステム上で任意のコードを実行できる可能性があります。

【検証結果】
下図は、攻撃後のターゲットシステムの画面です。これにより、ターゲットシステムを停止させることができます。

ターゲットシステムの停止に成功した画面



＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】
NTT データ先端技術株式会社
セキュリティ事業部
TEL:03-5859-5422
http://www.intellilink.co.jp/

Copyright © 2015. NTT DATA INTELLILINK CORPORATION All right reserved.