株式会社 日立システムズ

SSRC-VR-20150417

発行日:2015/04/17

S.S.R.C.

脆弱性検証レポート

(CVE-2015-1635)

株式会社　日立システムズ

セキュリティリサーチセンタ

© Hitachi Systems, Ltd. 2015- All rights reserved.

S.S.R.C.脆弱性検証レポート

目次

S.S.R.C.
Shield Security Research Center

© Hitachi Systems, Ltd. 2015 All rights reserved.

1. はじめに

S.S.R.C.(Shield Security Research Center)は、株式会社日立システムズ　セキュリティリサーチセンタが運営するセキュリティ情報公開サイトです。本サイトでは、セキュリティリサーチセンタによるリサーチ結果を随時配信する予定です。

本文書は、株式会社日立システムズ、SHIELD セキュリティセンタで日々収集を行っている世界中のセキュリティトレンド情報にもとづき、セキュリティリサーチセンタのセキュリティアナリストが確認した、ソフトウェア等の脆弱性検証結果をまとめたレポートです。

次に示す、ご利用条件を十分にお読み頂き、ご了承頂いた上でご利用頂きます様、よろしくお願い致します。

2. ご利用条件

本文書内の文章等すべての情報掲載に当たりまして、株式会社日立システムズ（以下、「当社」といいます。）と致しましても細心の注意を払っておりますが、その内容に誤りや欠陥があった場合にも、いかなる保証もするものではありません。本文書をご利用いただいたことにより生じた損害につきましても、当社は一切責任を負いかねます。

本文書に掲載されている情報は、掲載した時点での情報です。掲載した時点以降に変更される場合もありますので、あらかじめご了承ください。

© Hitachi Systems, Ltd. 2015 All rights reserved.

3. 概要

3.1. 脆弱性の概要

2015年4月15日(日本時間)、Microsoft社がHTTP.sys における脆弱性(CVE-2015-1635)を発表しました。[1]

この脆弱性を悪用されると、システムアカウントのコンテキストで任意のコードが実行される可能性があります。

3.2. 影響を受けるシステム

以下のソフトウェアに影響があります。

- Windows 7
- Windows Server 2008 R2
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 R2

3.3. 影響の有無の確認方法

脆弱性の影響有無を確認するための検証プログラムが公開されています。下記よりのソースコードをダウンロードし、コンパイルして実行して下さい。検証プログラム実行後、出力される文字列により影響有無の判別が可能です。

http://www.exploit-db.com/exploits/36773/

SSRC Shield Security Research Center

影響を受ける場合：

[!!]Looks VULN

影響を受けない場合：

[*]Looks Patched

3.4. 深刻度

深刻度:危険

CVSS 基本値:10.0 [NVD 評価]

© Hitachi Systems, Ltd. 2015 All rights reserved.

3.5. 対策方法

- 根本対策

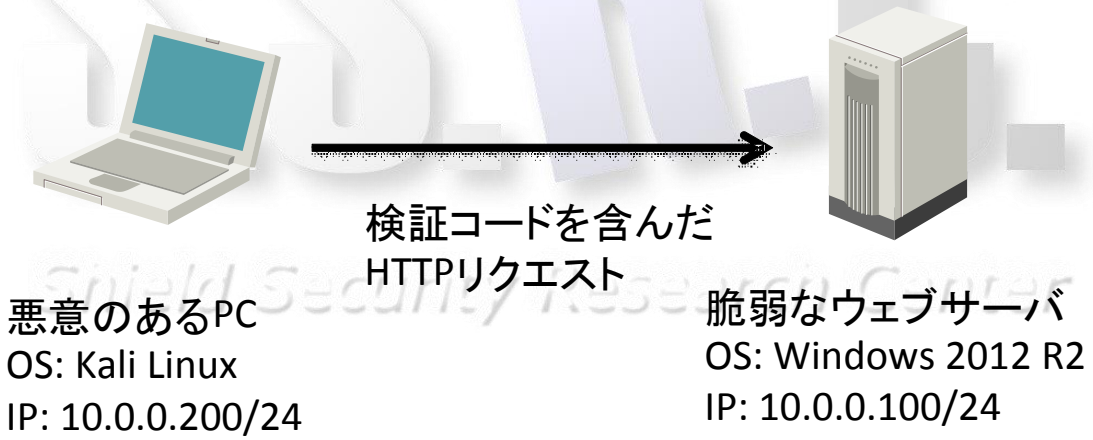
  Microsoft 社よりセキュリティ更新プログラム(MS15-034)が提供されています。
  Windows Update より、セキュリティ更新プログラム(MS15-034)を適用して下さい。

- 回避策

  IIS カーネル キャッシュを無効にする (IIS のみ有効な回避策) [2]
  パフォーマンスに影響が発生する可能性があるため、適用前に十分に検証されることを推奨します。

4. 検証

本検証のイメージは下記のとおりです。悪意のある PC (Kali Linux) から、脆弱なウェブサーバ (Windows2012 R2) に検証コードが含まれた HTTP リクエストを送信し、ウェブサーバの影響有無を検証します。本検証では、一般に公開されている情報源から集めた検証コードをもとに検証を実施しました。



© Hitachi Systems, Ltd. 2015 All rights reserved.

4.1. セキュリティ更新プログラム未適用環境での検証

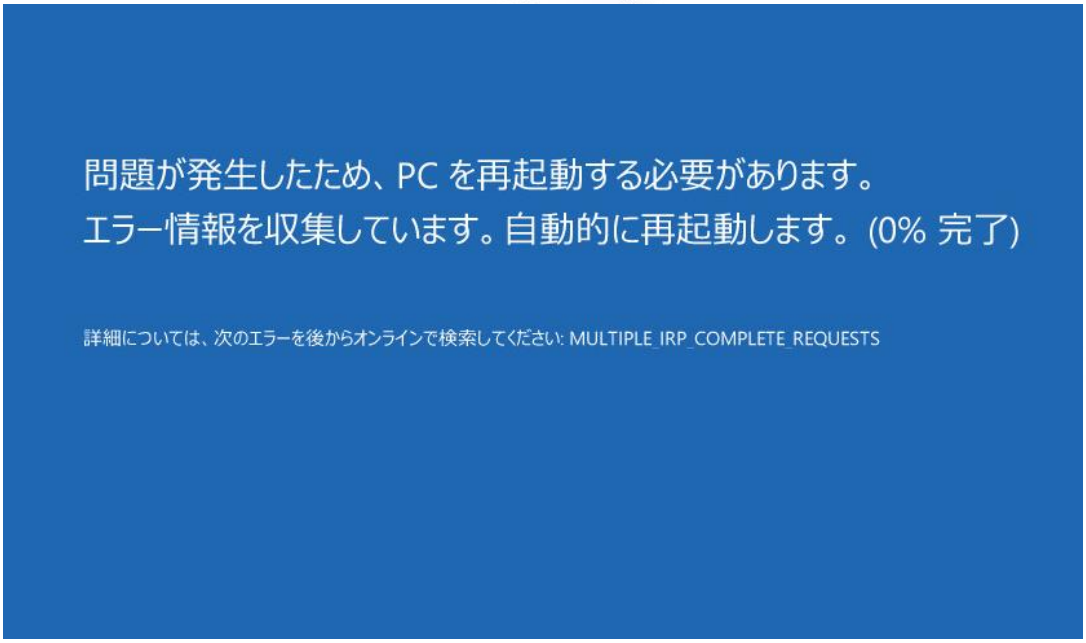
- **検証環境**

ウェブサーバ：

OS	: Windows Server 2012 R2 セキュリティ更新プログラム（MS15-034）未適用
Web サーバ	: IIS 8.0

- **検証結果**

下図は、検証コードが含まれた HTTP リクエストを受け付けたウェブサーバのコンソール画面です。本脆弱性を悪用され、ウェブサーバが停止・再起動状態になっていることがわかります。



© Hitachi Systems, Ltd. 2015 All rights reserved.

4.2. セキュリティ更新プログラム適用済み環境での検証

- **検証環境**

ウェブサーバ：

OS	: Windows Server 2012 R2 セキュリティ更新プログラム（MS15-034）適用済
Web サーバ	: IIS 8.0

- **検証結果**

「4.1 セキュリティ更新プログラム未適用環境での検証」と同様の手順で検証を実施しましたが、ウェブサーバが停止・再起動することはありませんでした。

4.3. IIS カーネルキャッシュ無効設定環境での検証

- **検証環境**

ウェブサーバ：

OS	: Windows Server 2012 R2 セキュリティ更新プログラム（MS15-034）未適用
Web サーバ	: IIS 8.0 IIS カーネルキャッシュ無効 [2]

- **検証結果**

「4.1 セキュリティ更新プログラム未適用環境での検証」と同様の手順で検証を実施しましたが、ウェブサーバが停止・再起動することはありませんでした。

© Hitachi Systems, Ltd. 2015 All rights reserved.

5. まとめ

セキュリティ更新プログラム未適用の環境ではシステムを停止させる攻撃が可能でしたが、セキュリティ更新プログラムを適用することで本脆弱性が修正されることを確認しました。

また、回避策として IIS カーネルキャッシュを無効に設定した環境では、攻撃が成立しないことを確認しました。ただし、この回避策は IIS のみに有効であり、パフォーマンスに問題を発生させる可能性があります。そのため、本回避策を適用する際には、十分に検証の上、適用されることを推奨します。

なお、本脆弱性は一行のコマンドを実行するだけで容易に攻撃が可能なため、今後、本脆弱性を悪用する攻撃が多発する可能性が高いと考えられます。当該製品をご利用の場合、早急に対策を実施されることを推奨します。

S.S.R.C.
Shield Security Research Center

[参考文献]

- ベンダ情報
  - [1] https://technet.microsoft.com/ja-jp/library/security/ms15-034.aspx
  - [2] https://technet.microsoft.com/ja-jp/library/cc731903(v=ws.10).aspx

- その他情報
  - [3] http://www.exploit-db.com/exploits/36773/
  - [4] https://ma.ttias.be/remote-code-execution-via-http-request-in-iis-on-windows/
  - [5] http://pastebin.com/raw.php?i=ypURDPc4

© Hitachi Systems, Ltd. 2015 All rights reserved.

S.S.R.C.

Shield Security Research Center

株式会社　日立システムズ
〒141-8672 東京都品川区大崎 1-2-1
http://www.hitachi-systems.com/index.html
http://www.shield.ne.jp/ssrc/index.html

© Hitachi Systems, Ltd. 2015 All rights reserved.