— AUS（アルテミス・ユーザ・サポート）便り 2016/11/07号 —
http://www.artemis-jp.com

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●「Security Essentials」をかたるマルウェア「Hicurdismos」が出現･･･Microsoftが注意喚起

http://forest.watch.impress.co.jp/docs/news/1026268.html
http://japan.zdnet.com/article/35091046/

このニュースをザックリ言うと･･･

- 10月21日（米国時間）、米Microsoft社より、同社のアンチウイルスソフト「Microsoft Security Essentials(MSE)」をかたるマルウェア「Hicurdismos」が出回っているとして、ブログにて警告が出されています。

- 記事によれば、「Hicurdismos」のインストーラはいわゆる「ドライブバイダウンロード」によって密かにPC上にダウンロードされ、これを誤ってインストールすることにより、偽のブルースクリーン画面（BSOD）が表示されます。

- そこには本物のBSODでは表示されない偽のサポート連絡先が記載されており、電話をかけることにより、「PCの問題を解決した」と偽ってサポート料を詐取しようとするとのことです。

AUS便りからの所感等

- MSEはWindows7以前向けのソフトで、Windows8以降ではデフォルトでアンチウイルスソフト「Windows Defender」が有効化されており、既に何らかのアンチウイルスをインストールしている限り、こういったものを新たにインストールする必要はありません。

- 今日、手元のPCに何のアンチウイルスも入っていないというのは論外ですが、それはさて置いて、どんなソフトウェアについても、信頼のおけるサイトからダウンロードし、ウイルススキャンを行った上でインストールすることは基本的なことです。

- また同社では、IEやEdge（Windows10の標準ブラウザ）に搭載されている「Smart Screen」機能を有効にすることにより、不正にダウンロードされることを抑止することが可能としており、そういったブラウザ・アンチウイルスの機能を一通り有効にし、かつUTMによる防御も確実に行うこと、そしてそれを行っていても普段からソフトウェアのダウンロード・インストールについては慎重になること、などが万が一のマルウェアの侵入を防ぐために大事なことです。

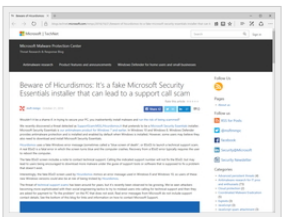
窓の社

「Security Essentials」を騙るマルウェア「Hicurdismos」が出現。Microsoftが注意喚起

偽のブルースクリーンを表示してサポート料を詐取

樽井 秀人　2016年10月24日 13:02

米Microsoft Corporationは21日（現地時間）、「Microsoft Security Essentials」を騙るインストーラー「Hicurdismos」が出回っていることを明らかにした。公式ブログ“Microsoft Malware Protection Center”に注意を喚起する記事を掲載している。



公式ブログ“Microsoft Malware Protection Center”

同社のブログ記事によると、「Hicurdismos」はWindows 7およびそれ以前のOS向けに無償提供している「Microsoft Security Essentials」のインストーラーを装って配布されており、誤ってインストールすると偽のブルースクリーン（BSOD）画面を表示する。この偽のブルースクリーン画面にはサポート連絡先（本物の画面には存在しない）が記載されており、コンタクトを取ると実際には存在しないPCの問題を解決したサポート料として金銭が請求される。

ZDNet Japan

マイクロソフト「Security Essentials」を装う新マルウェア「Hicurdismos」が登場

Liam Tung （Special to ZDNet.com） 翻訳校正： 編集部 2016年10月25日 10時20分

Microsoftの無料アンチウイルスソフトウェア「Microsoft Security Essentials」の偽インストーラについて、Microsoftが警告を発した。被害者をだまして偽のヘルプセンターに連絡させようとするものだ。

技術サポートを騙る詐欺師たちがその手法をさらに巧妙化させている。彼らが使用するのは、Security Essentialsを装い「Windows」を狙う新たなマルウェアだ。このマルウェアをインストールすると、エラーメッセージと、米国のフリーダイヤル（Microsoftのサポートセンターではない）に電話するよう促す一文を含む偽の死のブルースクリーン（BSoD）が表示される。

右が偽のメッセージ
提供：Microsoft

●「Red Hat Enterprise Linux」Ver.4/5が来年3月サポート終了

https://www.ipa.go.jp/about/press/20161101.html

このニュースをザックリ言うと・・・

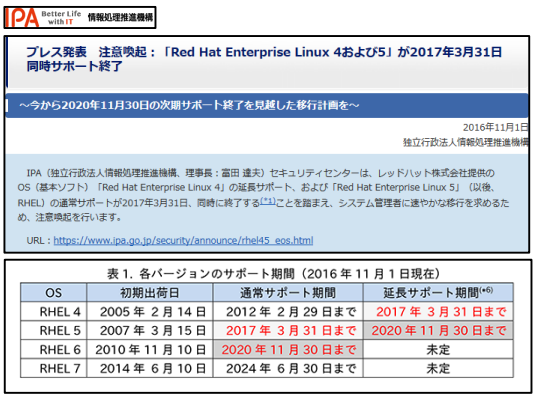
- 11月1日（日本時間）、情報処理推進機構（IPA）より、Linuxディストリビューション「Red Hat Enterprise Linux(RHEL)」のバージョン4および5が2017年3月31日をもってサポート終了することを受け、新しいバージョンへの移行を呼び掛けています。

- バージョン4はこの日をもって全てのサポートが終了、5は通常サポートの終了となり、引き続き延長サポートが2020年11月30日まで行われますが、パッケージの脆弱性対応は限定的なものとなる模様です。

- 現在、より新しいバージョンとしてRHEL 6および7がリリースされており、IPAでは特に7へのアップグレードを前提とした移行計画をとることを推奨しています。

AUS便りからの所感等

- アップグレードによる各種ソフトウェアのアップデートにより、構築したシステムが適切に動作しない可能性、また2つ以上先のバージョンへ一気のアップグレードは不具合が発生する場合がありますが、事前に十分な検証を行い、1つのバージョンずつアップグレードする形での移行計画を立てることが望ましいでしょう。


IPA 情報処理推進機構

プレス発表　注意喚起：「Red Hat Enterprise Linux 4および5」が2017年3月31日同時サポート終了

～今から2020年11月30日の次期サポート終了を見越した移行計画を～

2016年11月1日
独立行政法人情報処理推進機構

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）セキュリティセンターは、レッドハット株式会社提供のOS（基本ソフト）「Red Hat Enterprise Linux 4」の延長サポート、および「Red Hat Enterprise Linux 5」（以後、RHEL）の通常サポートが2017年3月31日、同時に終了する(*1)ことを踏まえ、システム管理者に速やかな移行を求めるため、注意喚起を行います。

URL：https://www.ipa.go.jp/security/announce/rhel45_eos.html

表 1. 各バージョンのサポート期間（2016 年 11 月 1 日現在）

OS	初期出荷日	通常サポート期間	延長サポート期間(*5)
RHEL 4	2005 年 2 月 14 日	2012 年 2 月 29 日まで	2017 年 3 月 31 日まで
RHEL 5	2007 年 3 月 15 日	2017 年 3 月 31 日まで	2020 年 11 月 30 日まで
RHEL 6	2010 年 11 月 10 日	2020 年 11 月 30 日まで	未定
RHEL 7	2014 年 6 月 10 日	2024 年 6 月 30 日まで	未定

- 最悪アップグレード自体が不可能と判断される可能性もありますが、この場合はOSが持つファイアウォール機能（iptables）をはじめとするセキュリティ機能を十分に設定し、UTMを隔てた隔離されたネットワークに配置することも検討すべきでしょう。

- RHELをベースとしている派生ディストリビューション「CentOS」も同様のサポートポリシーをとっており、やはり将来的なアップグレードが必要となることに注意してください。

●BINDに新たな脆弱性、3ヶ月連続の発表

https://jprs.jp/tech/security/2016-11-02-bind9-vuln-dname.html

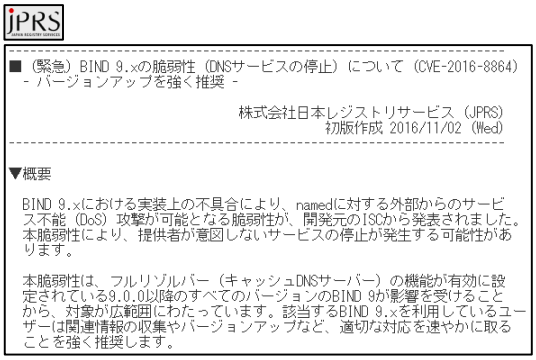
このニュースをザックリ言うと・・・

- 11月1日（日本時間）、DNSサーバーソフト「BIND」について1件の脆弱性（CVE-2016-8864）が発表、および開発元の米ISCより修正バージョン（BIND 9.11.0-P1/9.10.4-P4/9.9.9-P4）がリリースされ、これを受けて翌11月2日には、JPCERT/CCやJPRS等から警告が出されています。

- 脆弱性は、攻撃者が用意したDNSサーバに問合せを送信するよう誘導され、細工されたDNS応答を受信することにより、DNSサーバプロセス（named）を不正に落とされる可能性があり、BIND 9.0.0以降全てのバージョンに影響するため、BINDをDNSキャッシュサーバとして利用しているあらゆる組織について早急なアップデートが推奨されています。

AUS便りからの所感等

- BINDはインターネット上で最もよく利用されるDNSソフトウェアとされる一方、長年の傾向として、頻繁に脆弱性が発見・修正されており、特に今回の脆弱性の発表は、9月（「AUS便り 2016/10/03号」参照）、10月（「同2016/10/24号」参照）に引き続き3ヶ月連続となっています。


JPRS

■（緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2016-8864）
- バージョンアップを強く推奨 -

株式会社日本レジストリサービス（JPRS）
初版作成 2016/11/02（Wed）

▼概要

BIND 9.xにおける実装上の不具合により、namedに対する外部からのサービス不能（DoS）攻撃が可能となる脆弱性が、開発元のISCから発表されました。本脆弱性により、提供者が意図しないサービスの停止が発生する可能性があります。

本脆弱性は、フルリゾルバー（キャッシュDNSサーバー）の機能が有効に設定されている9.0.0以降のすべてのバージョンのBIND 9が影響を受けることから、対象が広範囲にわたっています。該当するBIND 9.xを利用しているユーザーは関連情報の収集やバージョンアップなど、適切な対応を速やかに取ることを強く推奨します。

- UTMをはじめ、Linuxベースのアプライアンス等でもよく利用されることがありますので、利用している機器にBINDが含まれているか、ファームウェア等の修正がリリースされているかメーカー情報をあたることが重要です。

- 今回の脆弱性はBINDをDNSキャッシュサーバ、即ち組織内から外部のWebサイト等の名前解決を行う目的で使用する場合に問題となりますが、外部から第三者がDNSキャッシュサーバを利用可能な設定になっている場合、攻撃者に容易に誘導される恐れがあり、この状態では偽のDNS情報をキャッシュさせられる等の攻撃を受ける可能性もあるため、組織内のIPアドレスからのみ利用可能であるよう設定を行うようにしてください。