— AUS（アルテミス・ユーザ・サポート）便り 2017/05/29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。

●メディアプレイヤーの字幕機能に脆弱性…2億人のPC・スマホが被害を受ける可能性

http://pc.watch.impress.co.jp/docs/news/1061654.html
http://gigazine.net/news/20170524-subtitle-file-hack-computer/

このニュースをザックリ言うと・・・

- 5月23日（現地時間）、大手セキュリティベンダーの米チェックポイント社より、動画をメディアプレイヤーソフトで字幕つきで再生する際の攻撃の可能性について、同社ブログにて警告が出されています。

- 同社によれば、VLCやKodi(旧・XBMC)・Popcorn Time・StremioといったPC・スマートテレビ・モバイル向けメディアプレイヤーソフトにおける字幕データの処理に脆弱性が存在し、不正に改変した字幕ファイルが読み込まれることにより、攻撃者が指定した任意のコードが実行される可能性があるとされています。

- ブログでは、「字幕データベースサイト上から不正な字幕ファイルを読み込んだPCを攻撃者がリモートから操作する」という攻撃のデモも示されています。

- 前述の各ソフトでは既に脆弱性が修正されたバージョンがリリースされており、アップデートが推奨されています。

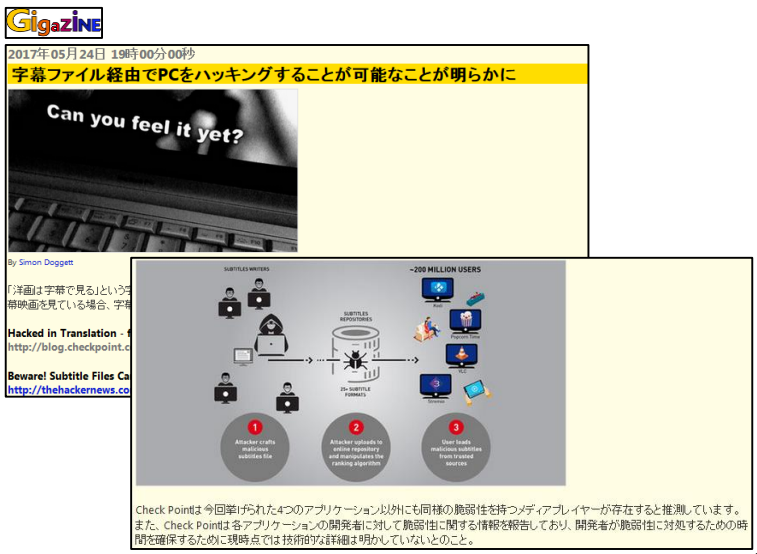
AUS便りからの所感等

- 攻撃のデモでは人気の字幕ファイルとして目に付きやすい場所に表示されるよう、攻撃者が事前の工作を行っている様子も示されています。

- 一例を挙げるならば、AndroidやiOS公式のアプリサイトに不正なアプリがアップロードされるケースと似通っていますが、ある字幕ファイルが本当に信用できる投稿者のものか等を事前に情報収集することは、より難しいものと考えられます。

- 今回のような事例が報告されたことにより、アンチウイルスソフトでの対応や、データベースサイトにおいての厳密なチェックが進むことが期待されますが、ともあれメディアプレイヤーソフトを最新のバージョンに保っておくことは欠かせません。

- ただし、一部ソフトのうちスマホ版のアプリについてまだアップデート版がリリースされていないものもあるため、その場合は脆弱性の対策まで字幕機能の使用を控えることも必要でしょう。



●「Samba」に重大な脆弱性、多くのファイルサーバに影響

http://www.itmedia.co.jp/enterprise/articles/1705/26/news048.html

このニュースをザックリ言うと・・・

- 5月24日（現地時間）、ファイルサーバソフトウェア「Samba」に重大な脆弱性（CVE-2017-7494）が報告されています。

- 脆弱性はSamba 3.5.0以降の全てのバージョンに存在し、共有フォルダへのデータ書き込みが可能な攻撃者により、サーバを乗っ取られる可能性があるとされています。

- Sambaの開発チームからは同日修正バージョン4.6.4、4.5.10、4.4.14がリリースされています。

AUS便りからの所感等

- SambaはLinux等UNIX系OSで利用される、WindowsのSMBと互換性のあるソフトウェアであり、NASアプライアンスの多くで使用されています。

- 先だって報告された「WannaCry」と同様、通常は外部から直接アクセスできず、別の経路で社内LANに侵入した攻撃者やマルウェアに狙われるケースが主でしょう。

- また、サーバのアーキテクチャーに適合した不正な共有ライブラリ（.so）ファイルを共有フォルダ上にアップロードできることが攻撃の条件とされています。

- Linuxマシン等にSambaをインストールしているケースにおいては修正バージョンへのアップデートを、一方、NAS等のアプライアンスについてはベンダーサイトにおいてファームウェアのアップデートの確認を、それぞれ必ず実施してください。


ITmedia エンタープライズ

「Samba」に重大な脆弱性、直ちに対処を

脆弱性はたった1行の攻撃コードで悪用できるといい、セキュリティ企業は「炎上の可能性もある恐ろしいバグ」と形容している。

[鈴木聖子，ITmedia]

UNIX系のOSとWindowsの相互運用に使われるオープンソースツール「Samba」に重大な脆弱（ぜいじゃく）性が報告され、修正のためのパッチが公開された。悪用が簡単にできてしまうことから影響が広範に及ぶ可能性も指摘され、セキュリティ機関などが迅速な対応を促している。

この問題を悪用すれば、公開のSMB共有（TCP 445番ポート）を見付けて共有ライブラリをアップロードする手口で、サーバにそれをロードさせ、実行させることができてしまう。セキュリティ専門家は、この脆弱性はたった1行の攻撃コードで悪用できると報告している。

影響を受けるのはSamba 3.5.0以降の全バージョン。脆弱性を修正したバージョン4.6.4、4.5.10、4.4.14が、5月24日に公開された。Sambaのセキュリティ情報ページでは回避策も紹介している。

SANSによると、SambaはNASなどのストレージ製品にも使われていることから、幅広いメーカーが影響を受ける可能性がある。セキュリティ企業のRapid7では、この脆弱性を「炎上の可能性もある恐ろしいバグ」と形容。悪用を狙ったスキャンが増大する形跡があり、コンセプト実証コードも出回っていることから、「ITチームは直ちに対処する必要がある」と呼び掛けている。

●WannaCryは序章？ NSAツールを悪用したマルウェアが相次ぎ出現

http://www.itmedia.co.jp/enterprise/articles/1705/23/news059.html

このニュースをザックリ言うと・・・

- 5月18日（現地時間）、セキュリティ企業のHeimdal Security社より、NSA（米国家安全保障局）から流出した攻撃ツールを利用した新たなマルウェアの存在が警告されています。

- 「EternalRocks(BlueDoom)」と呼ばれるマルウェアは、同社によれば5月上旬から確認されており、感染したPC上から外部とTorによる暗号化通信を行い、不正なファイルをダウンロードし、外部から制御可能な状態にするとされています。

- WannaCryのようなランサムウェア的なものではなく、感染と拡散以外の行動は確認されていませんが、より広範囲な感染活動の恐れがあるとして注意が呼びかけられています。

AUS便りからの所感等

- NSAから流出した攻撃ツールが悪用するWindowsの脆弱性は全てMicrosoftによって修正パッチがリリース済みのものであったにも拘らず、サポートが続いているOSですら被害を受けたPCが少なからず報告されていました。

- WannaCryが大きな騒ぎとなった今において、改めて十分な対策をとるよう手を打たなければ、次なる攻撃の犠牲となることは目に見えています。

- 何らかの理由でパッチが適用できないなどの問題を抱えているPCやサーバーについては、アンチウイルスの導入やUTMの設置による隔離を怠りなく行うのが重要です。


ITmedia エンタープライズ

WannaCryは序章？　NSAツールを悪用したマルウェアが相次ぎ出現

ネットワークワームの「EternalRocks」は、NSAのツールを長期的に悪用し、感染マシンを攻撃の発射台として利用する意図をもつ。

[鈴木聖子，ITmedia]

世界中で猛威を振るったランサムウェアの「WannaCry」。しかしこの攻撃と前後して、同じ米国家安全保障局（NSA）のハッキングツールを使った別のマルウェアの出現が報告されている。WannaCry以上の大規模攻撃を予想する見方もある。

NSAの悪用ツールはいずれも、ハッカー集団「Shadow Brokers」が4月に流出させた情報に含まれていた。

EternalRocksはWannaCryと違って、NSAのツールを長期的に悪用する意図があるとHeimdalは分析する。WannaCryのように標的をランサムウエアに感染させるのではなく、「現時点では今後の攻撃に向けた発射台の確立に重点を置いている」とみられる。

感染後24時間は休眠状態を保ち、続いてTorを利用して制御用サーバと通信。攻撃に必要なコンポーネントをダウンロードし、感染させたマシンを制御できる状態に置く。WannaCryと違って「キルスイッチ」も存在しないという。