— AUS（アルテミス・ユーザ・サポート）便り 2017/09/19号 —
https://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。

●ドコモのWi-Fiルータにバックドア…パッチ適用を

https://japan.zdnet.com/article/35107151/
http://k-tai.watch.impress.co.jp/docs/news/1080372.html

このニュースをザックリ言うと・・・

- 9月12日（日本時間）、情報処理推進機構(IPA)およびJPCERT/CCより、NTTドコモが販売しているモバイルWi-Fiルータ「Wi-Fi STATION L-02F」にバックドア等の問題があり、外部からルータに侵入され、マルウェアに感染する等の可能性があると発表されました。
  - IPA … https://www.ipa.go.jp/security/ciadr/vul/20170912-jvn.html
  - JPCERT/CC … http://www.jpcert.or.jp/at/2017/at170034.html
- JPCERT/CCでは7月の時点でTCPポート22番（SSHポート）への通信の増加を観測しており、今回ルータを踏み台としての攻撃である可能性を示唆しています。
- NTTドコモによれば、6月28日の時点でこれらを修正するパッチ（バージョンV10h）がリリースされており、速やかにパッチを適用するよう呼びかけています。

AUS便りからの所感等

- バックドアの他にも「外部からWeb管理画面にアクセスし、機器の情報を取得可能」という問題も発表されています。
- PCやスマートフォン・タブレットに比べ、ルータ等のネットワーク機器はファームウェアをアップデートすることへの意識が及びにくい傾向があり、特に当該ルータへのパッチ適用は手動で行う必要があるとのことです。
- 使用している全ての機器について、ベンダーサポート等の情報収集を定期的に行い、常に最新のバージョンに保つことを心がけるようにしましょう。

ZDNet Japan

ドコモのWi-Fiルータにバックドア問題や脆弱性--JPCERT/CCが注意喚起

ZDNet Japan Staff 2017年09月12日 17時33分

いいね！ 18　G+　B! 2　Pocket 25

印刷　メール▼　ダウンロード▼　クリップ

NTTドコモが提供するLG製のモバイルWi-Fiルータ「Wi-Fi STATION L-02F」でバックドアの問題と脆弱性が報告された。JPCERT コーディネーションセンター（JPCERT/CC）は、この問題によるとみられるサイバー攻撃を確認している。

バックドアの問題は、Wi-Fi STATION L-02Fのソフトウェアのバージョン V10gとそれ以前に存在する。この問題を悪用すれば、遠隔の第三者が管理者権限で製品にアクセスし、任意の操作を実行できてしまう。共通脆弱性評価システム（CVSS）v2を用いたこの問題の深刻度は、最大値の「10.0」と評価された。

JPCERT/CCでは、6月13日頃から国内のIPを通信元とする22/TCPポートへのアクセスを多数観測しており、特にモバイル回線からのアクセスが増加していた。JPCERT/CCは、この原因に今回の問題が関係しているとみている。問題を報告したJPCERT/CC 国際部 サイバーメトリクスライン 情報セキュリティアナリストの鹿野恵祐氏によれば、IDとパスワードを使って、インターネット経由で機器にログインし、任意のコマンドを実行できることを確認しているという。

この問題とは別に、Wi-Fi STATION L-02Fのソフトウェアのバージョン V10bとそれ以前に存在するアクセス制限不備の脆弱性も報告された。この脆弱性が悪用されると、遠隔の第三者によって、インターネット経由で製品のウェブインターフェースにアクセスされてしまい、設定情報を盗み取られる恐れがある。CVSS v2による深刻度は「5.0」と評価された。

ケータイ Watch

ドコモ「Wi-Fi STATION L-02F」にバックドアの脆弱性、悪用された通信を観測

6月のソフト更新で対応済み、ユーザーは更新の確認を

太田 亮三　2017年9月12日 14:40

ツイート　リスト　いいね！ 59　シェア　B! 8　Pocket 16

IPA（情報処理推進機構）は、NTTドコモが販売しているモバイルWi-Fiルーター「Wi-Fi STATION L-02F」（LG製）に複数のセキュリティ上の脆弱性があることを明らかにした。ドコモでは不具合を解消するソフトウェア更新を6月28日から提供している。同端末は自動更新には対応していないため、利用中のユーザーはソフトウェアバージョンの確認と更新が強く推奨される。

IPAが明らかにした「Wi-Fi STATION L-02F」の脆弱性情報は2件。1つめはアクセス制限不備の脆弱性があり、悪意のある第三者によって、遠隔操作で端末のWebインターフェイスにアクセスされ、機器の設定情報を取得される可能性があるというもの。ソフトウェアバージョンが「V10b」以前が影響を受ける。

2つめは、バックドアの問題が存在し、悪意[illegible]端末に管理者権限でアクセスされ、任意の操作[illegible]の。IPAでの報告では、実際に任意のコマンド[illegible]る。ソフトウェアバージョンが「V10g」以前[illegible]

「Wi-Fi STATION L-02F」→

●2017年上半期、添付ファイルを使ったサイバー攻撃手法に変化…警察庁調べ

https://www.is702.jp/news/2203/

このニュースをザックリ言うと・・・

- 9月7日（日本時間）、警察庁サイバー犯罪対策プロジェクトより、2017年上半期（1～6月）におけるサイバーセキュリティの脅威情勢についての分析結果が発表されました。
  - 警察庁 … http://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_kami_cyber_jousei.pdf

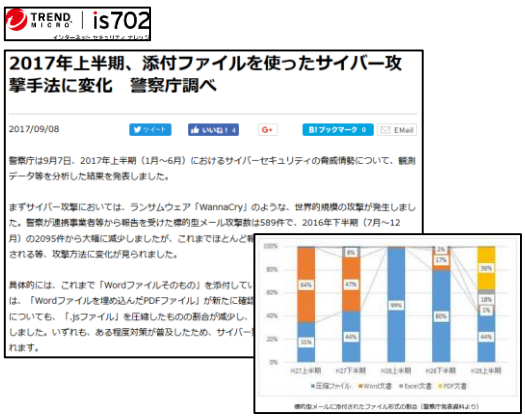
- 世界的規模の攻撃としてランサムウェア「WannaCry」が猛威をふるう一方、標的型攻撃メール件数は589件と、2016年下半期（7～12月）の2095件から大幅に減少しています。

- しかし、メールの添付ファイルとして「Wordファイルそのもの」だけでなく「Wordファイルを埋め込んだPDFファイル」が、また「.js(JavaScriptファイル)」に代わり「.wsf(Windowsスクリプトファイル)」を圧縮したものが、それぞれ多くみられるようになったとされています。

AUS便りからの所感等

- 不正なファイルを別の形式のファイル内に埋め込んでアンチウイルスを回避するやり方はもはや珍しくはありませんが、それでもあまり使われていない形式のファイルを悪用することにより、対応されるまでのタイムラグでの感染を狙うという意図があると思われます。

- とにかく、PC上のアンチウイルス、UTMによる通信のチェック等、複数の対策どれか一つに依存することなく、それぞれを確実に活用することがネットワーク全体をセキュアに保つために重要です。



●Bluetooth経由でスマホからPCまで乗っ取れる攻撃手法「BlueBorne」が発覚

http://pc.watch.impress.co.jp/docs/news/1080650.html

このニュースをザックリ言うと・・・

- 9月12日（現地時間）、IoTセキュリティ企業の米Armis社より、Bluetooth（以下BT）搭載デバイス（スマホ・PC等）に影響を与えるとされる複数の脆弱性が発表されました。

- 「BlurBorne」と名づけられた一連の脆弱性により、BTが稼動している機器に対し、リモートの攻撃者がペアリングを行っていなくてもBT経由でアクセスすることができ、情報を盗み出されたり、機器を乗っ取られたりする恐れもあるとされています。

- AndroidではGoogleより6.0, 7.0向けパッチがリリースされ、Windowsでも9月13日（日本時間）発表のセキュリティパッチで対策されているほか、iOSはバージョン9.3.5以前に影響するとされており、影響を受けないバージョン10へのアップデートが推奨されています。

AUS便りからの所感等

- BluetoothはWi-Fiに比べアクセス可能な範囲が狭いプロトコルであることから、「実際に攻撃される可能性は低い」ものと油断するユーザもいるかもしれませんが、複数のBTが稼動している機器同士で連鎖して攻撃を受けることにより、想像以上に広範囲に攻撃が拡散する可能性も指摘されています。

- Androidではそれ自体にはパッチがリリースされているものの、各社製品にパッチが確実に行き渡るには時間がかかるとみられており、パッチが適用でき、安全であることが確認できない限り、BTを使わないようにすることも視野に入れるべきでしょう。