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。

●バッファロー製ルーター等一部製品に脆弱性…サポート終了済み、使用停止呼び掛け

https://k-tai.watch.impress.co.jp/docs/news/1322908.html
https://www.buffalo.jp/news/detail/20210506-01.html
https://jvn.jp/vu/JVNVU90274525/

このニュースをザックリ言うと･･･

- 4月27日(日本時間)、バッファロー社より、同社が販売していたネットワーク製品に脆弱性が存在していたとして注意喚起が出されています。

- 脆弱性の内容は、製品に存在するデバッグオプションを有効化されるというもので、同社によれば、「当該商品にアクセス可能な攻撃者により、デバッグ用Webページにアクセスされ、機微な情報を窃取されたり、任意のコード実行や設定の書き換えが行われたり、機能を停止させられたりする可能性」があるとしており、また同じく4月27日に出されたIPA・JPCERT/CCからの注意喚起でも「隣接するネットワーク上の第三者」が機器にアクセスする可能性が想定されるとしています。

- 対象製品はいずれもサポート終了済みで、Wi-Fiルーターをはじめ、無線ブリッジ・有線ルーターおよびイーサネットコンバーターも含まれており、各注意喚起では該当する商品の品番を提示するとともに、各製品の使用を停止し、代替品への移行を推奨しています(一部バッファロー社から後継機種が案内されているものもあります)。

AUS便りからの所感等

- IPA・JPCERT/CCの注意喚起において想定されている可能性の内容から、外部ネットワークから無条件に悪用こそできないものの、組織の内部ネットワークにまで侵入した攻撃者であれば、管理画面の認証による制限等もなく、ルーター等を乗っ取ることは容易であると考えられます。

- 対象製品の多くは2000年代前半に発売され、最新のファームウェアのリリースからも10～15年以上経過しているものですが、現時点でもこのような機器が使い続けられている場合は、故障するまで使い続けられるケースや、クライアント・サーバーPCと異なり、ファームウェアのアップデートを適用する等の管理が行き届いていないケース、さらには管理対象として認識されないケースすらあるものと推察されます。

- 家庭・企業に拘わらず、使用している各ネットワーク機器について、機種を含め把握・管理するとともに、ファームウェアのアップデート等のサポートがされなくなった場合を考慮し、機器交換を計画的に行うことが重要です。

Impress Watch

バッファローの一部Wi-Fiルーターなどに脆弱性、「製品の使用停止」を推奨

竹野 弘祐　2021年5月7日 12:10

JVNサイトより

JPCERTコーディネーションセンターと情報処理推進機構（IPA）は、バッファロー製の複数のネットワーク機器で、「第三者によりデバッグ機能が有効化される」脆弱性の情報を公開した。

対象のネットワーク機器は、Wi-Fiルーター「WBR-B11」、「WBR-G54」、「WBR-G54L」、「FS-G54」など19製品と無線ブリッジ「WLA2-G54」、「WLA2-G54C」など8製品、有線ルーター「BHR-4RV」、イーサネットコンバーター「WLI-T1-B11」など7製品。

●4月度フィッシング報告件数は44,307件、今後も同水準維持か…対策協議会発表

https://www.antiphishing.jp/report/monthly/202104.html

このニュースをザックリ言うと・・・

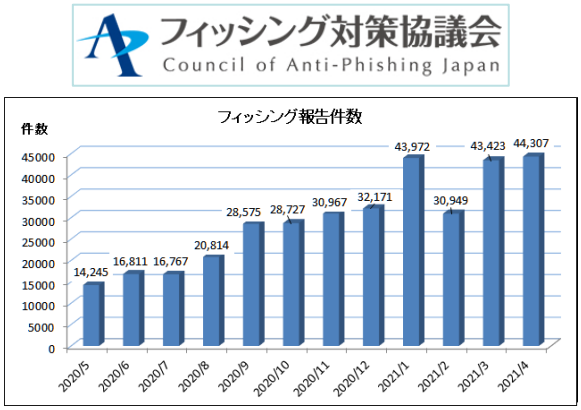
－5月7日(日本時間)、フィッシング対策協議会より、4月に同協議会に寄せられたフィッシング報告状況が発表されました。

－4月度の報告件数は44,307件で、3月度(https://www.antiphishing.jp/report/monthly/202103.html)の43,423件から884件の増加となり、1月度(https://www.antiphishing.jp/report/monthly/202101.html)に記録した43,972件に近い水準を維持しています。

－フィッシングメールに悪用されたブランドについては、報告全体に対するAmazonの割合が50.7%、これに楽天・三菱UFJニコス・三井住友カード・JCBを合わせた5ブランドで約81.2%を占めているとのことです。

AUS便りからの所感

－同協議会への毎月のフィッシング報告件数は、2021年1月度に前月度までの3万件台から4万件台へと急増、2月度に一時的に落ち込んだのを除いて同水準を維持している他、2019年以降をみても右肩上がりの傾向を持続しており、今年中に5万件台前後となることも十分に考えられます。



－フィッシングの全体的な傾向は先月度と概ね変わりなく、クレジットカード以外にも、仮想通貨(暗号資産)・ISP・ホスティング事業者や宅配業者の不在通知を騙るメール・SMSによるフィッシングが挙げられ、この他にユーザーのプライバシーを盗み見ていると偽って仮想通貨を要求する脅迫メール(セクストーション)についても注意喚起が出されています。

－今後も、同協議会や各セキュリティ関連団体等の啓発、利用しているサービス等からの公式発表あるいはソーシャルネットワーク上で報告されている情報等に注意を払い、信頼できないメール・SMSのリンクはクリックせず、サービスの公式サイトにはブックマークからアクセスするよう努める等、フィッシングをはじめとする各種攻撃に対応できるよう慎重な行動をとって頂ければ幸いです。

●東京都のワクチン接種予約サイトに不具合、27万人分の個人情報が閲覧可能状態に

https://www.jiji.com/jc/article?k=2021042700879&g=pol
https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/04/28/20.html
https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/05/07/12.html

このニュースをザックリ言うと・・・

－4月27日(日本時間)、東京都福祉保健局より、都内の医療従事者等向けに開設したワクチン接種予約サイトにおいて、個人情報が閲覧可能な不具合が存在していたことが発表されました。

－予約サイトでは同26日から予約受付を開始していましたが、接種予定者27万人の個人情報(氏名・生年月日・職種・接種券番号)が特定の操作によって閲覧可能になるという不具合について連絡を受け、同27日未明にシステムの予約機能を停止したとしています。

－その後システムの改修が行われ、5月11日に再開予定とされています。

AUS便りからの所感

－都の発表では、本来は受け付けていない接種枠について、1,023人分の予約を誤って受け付けるという別の不具合についても明らかになっており(こちらも現在修正済みとのことです)、他にもアクセスが集中して繋がりにくい状態となっていたという報告もネット上ではあった模様です。


報道発表資料　2021年04月27日　福祉保健局

ワクチン接種予約システムの不具合について

令和3年4月26日午前9時00分から医療従事者等向けの接種予約を開始したホームページの「ワクチン接種予約システム」に関して、次の2点の不具合があることが判明しました。関係者の皆様に多大なるご迷惑をおかけしたことを深くお詫び申し上げます。

1　個人情報の扱いに係る不具合

経緯

› 4月27日午前1時30分頃
都民から、特殊な解析ツールを用いて、システムに特定の操作を行うと接種予約者の個人情報（氏名・生年月日・職種・接種券番号）が閲覧可能であるため、早急な対応をすべきとの情報提供があった。

› 午前2時00分
都は、運用事業者に連絡し、一時的にシステムの予約機能を停止した。

› システムには接種予定者27万人の医療関係者の情報が登録されている。個人情報に係るシステム改修が完了するまでシステムは中止し、コールセンターでの予約対応とする。また、システムでコールセンターへの誘導を行っている。

› なお、上記操作を用いたアクセスの有無については、現在、調査中である。

－「特殊な解析ツールを用いて、システムに特定の操作を行う」ことで個人情報が閲覧可能という、Webアプリケーションにおいて何らかの脆弱性が存在する状態だった模様ですが、特に不特定多数がアクセス可能なWebサイトにおいては、このような手法で脆弱性を突こうとする攻撃者がアクセスしてくることを想定し、第三者機関による十分な診断を受け、より早い段階で脆弱性の対策を行っておくことが肝要です。