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。

●同人向けSNS等に不正アクセス、アカウント情報等流出…パスワード使い回しの場合は変更を

https://www3.nhk.or.jp/news/html/20230816/k10014164881000.html
https://forest.watch.impress.co.jp/docs/news/1524162.html
https://piyolog.hatenadiary.jp/entry/2023/08/17/030141

このニュースをザックリ言うと･･･

- 8月15日(日本時間)、同人向けSNS「pictBLand」、オンライン即売会サービス「pictSQUARE」等の運営会社より、同2サービスが不正アクセスを受け、アカウント情報等が流出したと発表されました。

- 同21日の続報によれば、被害を受けたのは両サービス合わせてアカウント情報801,915件、メールアドレス608,967件、電話番号670,241件、住所221,007件、銀行口座情報：883件およびTwitter(現X)のID 240,686件とされています(クレジットカード情報は含まれていないとのことです)。

- 同社ではパスワードも流出した可能性があるとしており、同サービスと同じパスワードを外部のサービスで使用していた場合は変更すること、不審なメール・SMSが届いた場合にリンクをクリックしないこと、登録されていた銀行口座に不審な入金があった場合は銀行に確認することを呼び掛けています。

AUS便りからの所感等

- 同16日にはアカウント情報を奪取したとみられる人物が攻撃者フォーラムに投稿を行ったという情報があり、パスワード情報はMD5による単純なハッシュ化がされており、多くが元のパスワードを割り出せていたとの証言があった模様です。

- 流出したID(メールアドレス)とパスワード情報で他のWebサービスへの不正ログインを行う攻撃は既にメジャーな手法であり、今回の発表を受けてPixiv等同種のWebサービスでもパスワードの使い回しをしていないか確認するよう呼び掛けています。

- Twitterアカウントの乗っ取りによるとみられる不正な投稿も多数発生しており、Twitterのパスワードの確認はもちろん、TwitterにてpictBLand・pictSQUAREと連携を行っていた場合にそれを悪用される恐れがあるため、連携を解除することを強く推奨致します。

- また、Webサービスあるいは各種サーバーの管理においてパスワードを保存する場合も、パスワードそのものを平文で保存するのは論外として、ソルト(ランダムな文字列を付加してからハッシュ化)やストレッチング(ハッシュ化を複数回行う)といったハッシュ化された文字列が奪取された場合にもパスワードの割り出しまでに時間がかかるようにする保存手法をとることが推奨されていますが、そういった手法を独自に実装することはせず、既成のソフトウェアを使用することが肝要です。

NHK

pictBLandなど運営会社 不正アクセスで個人情報漏えいのおそれ

2023年8月16日 18時53分　IT・ネット

SNSの「pictBLand」などを運営する名古屋市の会社は、データベースに不正アクセスがあり、ユーザーのメールアドレスやパスワードなどが漏えいしたおそれがあると発表しました。

ユーザーの情報が漏えいしたおそれがあるのは、SNSサービスなどを展開する名古屋市の「GMW」です。

会社によりますと14日ごろから運営するサービスのウェブサイトを閲覧しようとすると不正なサイトにつながる現象が発生し、調べたところ、データベースに対し、不正アクセスが行われ、情報が漏えいしたおそれがあることがわかったということです。

●エレコム製Wi-Fiルーターに脆弱性…サポート切れ機種はリプレース推奨

https://www.itmedia.co.jp/news/articles/2308/10/news126.html
https://www.elecom.co.jp/news/security/20230810-01/
https://www.elecom.co.jp/news/security/20230711-01/

このニュースをザックリ言うと･･･

- 8月10日(日本時間)、エレコム(ELECOM)社より、同社および子会社のロジテック(Logitec)社が発売した一部のWi-Fiルーター等ネットワーク機器に、脆弱性が存在すると発表されました。
- 脆弱性の悪用により、任意のコマンドを機器上で実行する等、機器の乗っ取りに繋がる攻撃が可能になるとされており、IPA・JPCERT/CCからも注意喚起が出されています(エレコム社の発表ページからリンクされています)。
- 同社では、対象製品はいずれも2017年2月以前の発売で、アップデートサービスはすでに終了しているとし、代替製品への切り替え等を行うよう呼び掛けています。

AUS便りからの所感

- 同社では7月11日に他の機種で類似した脆弱性に対するセキュリティアップデートをリリースしており、今回の発表は同様の脆弱性がサポート切れの機種にも存在することについてのものとみられます。
- 「ELECOM」「Logitec」各ブランドの機器を使用しているユーザー・組織においては、前述した二度の発表情報を速やかに参照し、対象となる機器・セキュリティアップデートの有無を確認の上、適宜対応を行うようにしてください。
- 今回対象となる機器には筐体から品番が確認できない機種も多く、組織内の機器管理の際は品番・形状・設置場所等を詳細に記録することが、サポートが終了したり年数が経過したりした機器を計画的に更新する体制の一助となることでしょう。

ITmedia NEWS

エレコム、過去発売のWi-Fiルーターに脆弱性　更新期間終了済み、“買い替え”推奨　「力及ばず謝罪しかできない」

2023年08月10日 13時40分 公開　［松浦立樹，ITmedia］

エレコムは8月10日、過去に販売していた一部Wi-Fiルーターに脆弱性が見つかったと発表した。対象製品は2017年2月以前に発売したもので、いずれもすでにアップデートサービスを終了している。悪用された場合、攻撃者によって任意のコマンドが実行される可能性があるため、同社は代替製品への切り替えを勧めている。

対象製品は15年9月～17年2月に発売したエレコムブランドの14製品と、子会社のロジテックが09年10月～13年5月に発売した12製品。製品発売当時には存在しなかった脆弱性であり、すでにアップデートサービスの期間を終えているため、別の製品への交換（買い替え）でしか対応できないとしている。

● Wi-Fi対応プリンターの設定情報が完全に初期化されない可能性…キヤノンが注意喚起

https://pc.watch.impress.co.jp/docs/news/1520974.html
https://psirt.canon/advisory-information/cp2023-003/

このニュースをザックリ言うと･･･

- 7月31日(現地時間)、キヤノンのグローバルサイトにて、同社製のWi-Fi対応インクジェットプリンターに保存されるWi-Fi接続情報に関する注意喚起が出されています。
- 家庭用・オフィス用の大判プリンターの特定機種で、単に設定を初期化しただけではWi-Fi接続情報が削除されない場合があるとされています。
- 対策として、「すべての設定を初期化→無線LANを有効化→再度すべての設定を初期化」の手順をとること、またすべての設定を初期化する項目がない機種の場合は「LAN設定の初期化→無線LANを有効化→再度LAN設定を初期化」することが挙げられています。

AUS便りからの所感

- 注意喚起は英語で発表されており、対象となる機器のリストは「Please check the affected inkjet printer models from here.」の部分からリンクされているPDFを参照してください。
- 今回は工場出荷時状態へ初期化する機能において情報が完全に消去されないケースが発覚したという特殊な事例となりましたが、ともあれ各種ネットワーク機器からPC・スマートフォン等に至るまで、再利用が可能な状態で廃棄された際に保存されている機密情報が露呈しないよう、初期化を行うことを大前提とすることが重要です。

Impress Watch

キヤノン製インクジェットプリンタにWi-Fi設定が初期化されない脆弱性

関根 慎一　2023年8月2日 11:22

Canon PSIRTは7月31日、同社製インクジェットプリンタで初期化操作をした際に、Wi-Fiの接続設定が削除されずに残る場合があるとして注意喚起を行なった。

特定モデルのホーム/オフィス/大判プリンタで発生する不具合。プリンタを修理/破棄/貸出/売却する際などにセキュリティ上のリスクとなる可能性がある。キヤノンではこの脆弱性が存在する製品のリスト(または下記参照)を公開している。