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。

●Githubにデータサーバーへのアクセス情報…自動車用ネットサービスユーザー296,019件のメールアドレスが閲覧可能状態

https://www.itmedia.co.jp/news/articles/2210/07/news178.html
https://global.toyota/jp/newsroom/corporate/38095972.html

このニュースをザックリ言うと･･･

- 10月7日(日本時間)、トヨタ自動車より、同社製自動車用コネクティッドサービス「T-Connect」一部ユーザーの情報が外部に漏洩した可能性があると発表されました。

- 対象となるのは、2017年7月以降に同サービスのユーザーサイトに登録した296,019件のメールアドレスおよび管理用の番号で、氏名・電話番号・クレジットカード番号等は含まれないとのことです(レクサス車向け「G-Link」「G-Link Lite」および「MyTOYOTA」「My TOYOTA+」アプリについて登録したメールアドレスも対象外とされています)。

- 2017年12月にユーザーサイトの開発委託業者が、データサーバーへのアクセスキー等が含まれたソースコードの一部をソースコード共有サイト「GitHub」に公開状態でアップロードしており、これを閲覧した第三者が外部からサーバーにアクセスし、データを取得することが可能な状態にあったとしています。

- 同社では9月15日に上記の事実を確認、直ちにソースコードを非公開化させ、同17日にアクセスキー変更の対応を行ったとしています。

AUS便りからの所感等

- 同社では、対象となるメールアドレスの不正利用は現在確認されていないものの、メールアドレスを悪用したなりすまし・フィッシングメール等が送信される可能性があるとして注意を呼び掛けており、例えば今回の件でパスワード変更を要求するメールが届いた場合は間違いなくフィッシングとみて良いでしょう。

- GitHubに内部・外部のサーバーやAWS等クラウドサービスのアカウント情報を含んだソースコードがアップロードされる事故は枚挙にいとまがありませんが、単純にGitHub等の利用を禁止することが全てにおいて最良の安全策となるとは限らず、過去に発生した同様のセキュリティ事故の事例をもとに適正なサービスの利用を徹底するよう教育することも重要でしょう。

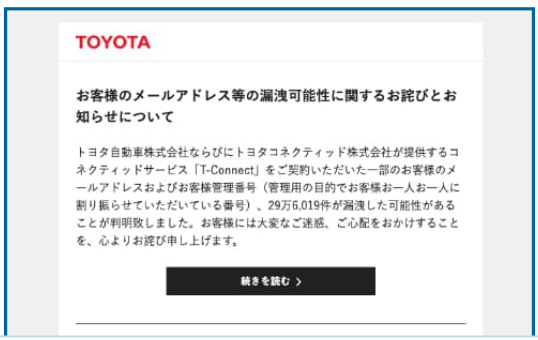
- データサーバーに対しては、アクセスキーの有無に拘わらず、Webサーバー以外の外部ネットワークからも接続が可能になっていたものと推測され、多重防御策として、IPアドレスベースでのアクセス制限等についても可能な限り実施すべきです。

ITmedia NEWS

トヨタ、ユーザーのメアド約30万件漏えいの可能性 ソースコードの一部、GitHubに5年間放置

2022年10月07日 16時52分 公開 [ITmedia]

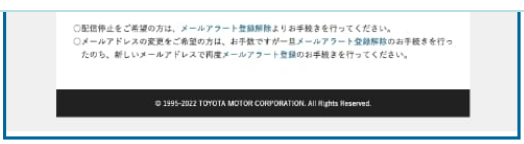
トヨタ自動車は10月7日、クルマ向けネットワークサービス「T-Connect」ユーザーのメールアドレスと「お客様管理番号」、29万6019件が漏えいした可能性があると発表した。


TOYOTA

お客様のメールアドレス等の漏洩可能性に関するお詫びとお知らせについて

トヨタ自動車株式会社ならびにトヨタコネクティッド株式会社が提供するコネクティッドサービス「T-Connect」をご契約いただいた一部のお客様のメールアドレスおよびお客様管理番号（管理用の目的でお客様お一人お一人に割り振らせていただいている番号）、29万6,019件が漏洩した可能性があることが判明致しました。お客様には大変なご迷惑、ご心配をおかけすることを、心よりお詫び申し上げます。

続きを読む ›


○配信停止をご希望の方は、メールアラート登録解除よりお手続きを行ってください。
○メールアドレスの変更をご希望の方は、お手数ですが一旦メールアラート登録解除のお手続きを行ったのち、新しいメールアドレスで再度メールアラート登録のお手続きを行ってください。

© 1995-2022 TOYOTA MOTOR CORPORATION. All Rights Reserved.

トヨタがユーザー向けに送信した謝罪と注意喚起のメール

2017年7月以降にT-Connectユーザーサイトにメールアドレスを登録した人が該当する。氏名や電話番号、クレジットカード番号などが漏えいした可能性はないという。

原因は2017年12月にT-Connectユーザーサイトの開発委託先企業が、取り扱い規則に反してソースコードの一部を誤って公開設定のままGitHubアカウントにアップロードしたこと。その後、5年にわたって第三者がソースコードの一部にアクセスできる状態で放置されていた。ソースコードにはデータサーバへのアクセスキーが含まれ、これを利用するとサーバに保管しているメールアドレスやお客様管理番号にアクセスできたという。

● 9月度フィッシング報告件数は102,025件…7月度以来の10万件超え

https://www.antiphishing.jp/report/monthly/202209.html

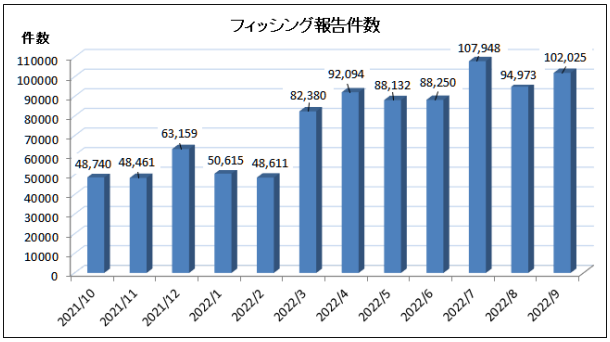
このニュースをザックリ言うと・・・

- 10月6日(日本時間)、フィッシング対策協議会より、9月に寄せられたフィッシング報告状況が発表されました。
- 9月度の報告件数は102,025件で、8月度(https://www.antiphishing.jp/report/monthly/202208.html)の94,973件から7,052件増加し、7月度(107,948件)以来再び10万件を超えています。
- フィッシングサイトのURL件数は53,612件と、8月度(49,221件)から4,391件の増加で、3か月連続の過去最高更新となっています(ただしIPアドレスとしては35アドレス程度とのことでした)。
- 同協議会が6月に緊急情報を出していた「クレジットカードの利用確認を装うフィッシング」が報告数全体の約38.7%を占め、VISA・セゾンカード・JCBを騙るものが特に多く報告されており、次いで報告が多かったAmazon・三井住友銀行・イオンカードを騙るフィッシングと合わせると全体の約68.8%に上るとしています。

AUS便りからの所感

- フィッシング報告件数の過去の傾向から、今後しばらく10万件前後で増減を繰り返した後、突如急増してより高い水準の件数となるものと予想されます。
- フィッシングサイトで使用されるTLD(トップレベルドメイン)の割合は、.topが約38.8%でトップ、次いで.icuが約20.9%、以下.shop、.com、.xyz、.cn、.cyou、.barが上位に挙げられています。
- 8月に報告されたGoogle翻訳の正規URLから誘導されるフィッシングが増加傾向にあり、かつURLフィルターで警告が出ないケースもあるとされていることから、特に注意が呼び掛けられています。
- 同協議会では、事業者(オンラインサービス等を提供する事業者orその他企業・団体)と個人のユーザーそれぞれに対しフィッシングへの様々な対策を推奨しており、個人ユーザーにおいては、不審なメールやSMSを受信した場合に同協議会や企業からの警告あるいはソーシャルネットワーク等での報告がないか確認し、サービスへのアクセスやログインについては事前に登録したブックマークから行うことを徹底することが、フィッシングによる個人情報等の詐取から身を守るために重要です。

フィッシング対策協議会 Council of Anti-Phishing Japan



●バッファロー製Wi-Fiルーターに乗っ取り可能な脆弱性…ファームウェア更新か使用停止を

https://pc.watch.impress.co.jp/docs/news/1444685.html
https://www.buffalo.jp/news/detail/20221011-01.html
https://jvn.jp/vu/JVNVU92805279/

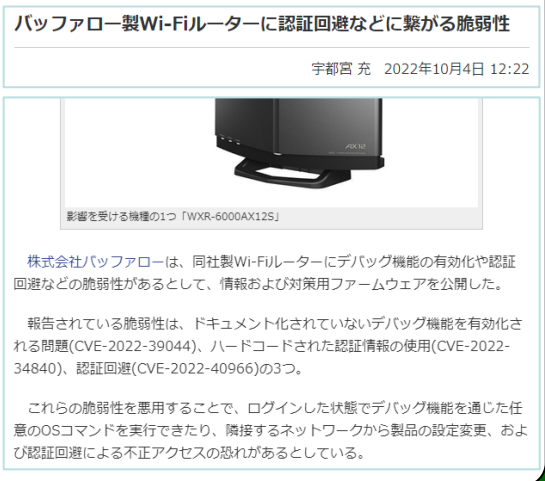
このニュースをザックリ言うと・・・

- 10月3日(日本時間)、バッファロー社より、同社が販売しているWi-Fiルーター等ネットワーク製品の一部に脆弱性が存在しているとして注意喚起が出されています。
- 脆弱性の悪用により、攻撃者に任意のOSコマンドをルーター上で実行される等、ルーターの乗っ取りが可能とされています。
- 同社Webサイトでは各種脆弱性の対象となる商品を掲示、一部製品についてファームウェアのアップデートを提供しています。
- ただしサポートの終了によりアップデートが提供されない製品もあり、これらについては使用を停止し、新商品へ移行することを推奨しています。

AUS便りからの所感

- 同4日にはJPCERT/CCからも注意喚起が出され、「隣接するネットワーク上の第三者」から攻撃を受ける可能性があるとされており、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、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。
- また「Internet側リモートアクセス設定を許可する」設定が有効な場合、外部から直接攻撃を受ける恐れがあるとされ、当該設定は通常無効化することを強く推奨致します。
- 対象となる機種のうちファームウェアのアップデートが提供されているものは殆ど2009年以降に発売されたものに限られており(例外もあり)、それより前の古い機種は故障するまで使い続けられたり、ファームウェア更新を含めた管理が行き届いていない可能性もありますので、家庭・企業に拘わらず、使用されている各ネットワーク機器について機種を含め把握・管理し、機器交換についても計画的に行えるような体制を整えることが肝要です。

Impress Watch


バッファロー製Wi-Fiルーターに認証回避などに繋がる脆弱性

宇都宮 充　2022年10月4日 12:22

影響を受ける機種の1つ「WXR-6000AX12S」

株式会社バッファローは、同社製Wi-Fiルーターにデバッグ機能の有効化や認証回避などの脆弱性があるとして、情報および対策用ファームウェアを公開した。

報告されている脆弱性は、ドキュメント化されていないデバッグ機能を有効化される問題(CVE-2022-39044)、ハードコードされた認証情報の使用(CVE-2022-34840)、認証回避(CVE-2022-40966)の3つ。

これらの脆弱性を悪用することで、ログインした状態でデバッグ機能を通じた任意のOSコマンドを実行できたり、隣接するネットワークから製品の設定変更、および認証回避による不正アクセスの恐れがあるとしている。