2021年6月23日

TABICAユーザー各位

個人情報漏えいの可能性についてのお詫びとお知らせ

このたび、TABICAにおいてサイトの脆弱性についてユーザーから報告を受け、内部で確認を行ったところ第三者がユーザー情報を閲覧するAPIを経由して特定の項目が閲覧できることが発覚しました。それに対する調査ならびに対応を公表します。

過去本件による個人情報漏えいがあったか調査を行いましたがアクセスログから判別することは困難であり、個人情報漏えいの事実を確認することができませんでした。

脆弱性に関しては既に対応が完了しており、現時点での被害報告はございません。

なお、今回の公表以降にTABICAからユーザーに対して個人情報を聞き出す、パスワード等の変更を要求するなどの個別連絡は一切致しません。TABICAになりすました連絡にはご対応されませんようご注意ください。

このたびはユーザーや関係者の皆様に多大なるご迷惑とご心配をおかけする事態となり、心よりお詫び申し上げます。今後は再発防止の対策を徹底してまいります。今回の経緯と内容および対策につきまして、下記のとおりご報告致します。

記

1.経緯

2021年6月18日 17:43

ユーザーより、ユーザー情報を閲覧するAPIを経由して任意のユーザーIDの情報を閲覧できる旨報告がありました。

2021年6月18日 17:54

内部的な調査を行ったところ、ユーザーの指摘にあるように、任意のユーザーIDの「本名」「メールアドレス」「電話番号」「フリガナ」の項目が特殊なアクセスにより閲覧できることが判明しました。

2021年6月18日 20:48

ユーザー情報のうち、「メールアドレス」を閲覧できなくするための修正を実施しました。

2021年6月21日 14:13

ユーザー情報のうち、「本名」「電話番号」「フリガナ」を閲覧できなくするための修正を実施しました。

2021年6月21日 17:27

影響範囲に関する調査を行い、脆弱性の存在した期間、脆弱性の利用された形跡について調査を行いました。

2.調査結果

脆弱性が存在した期間

本名 (2019年6月12日-2021年6月21日)

メールアドレス(2020年1月15日-2021年6月18日)

電話番号(2020年1月15日-2021年6月21日)

フリガナ(2019年10月9日-2021年6月21日)

脆弱性が利用された形跡

脆弱性を利用するためには、ユーザー情報を閲覧するAPIを経由する必要があります。脆弱性を利用したAPIへのアクセスをログから調査を行いましたが、正常な実行と不正な実行とを区別することができず攻撃の形跡を確認することはできませんでした。

影響範囲（最大）

ログから不正な攻撃パターンが特定できなかったため、現時点での最大の漏えい可能性はそれぞれ以下の通りです。

本名 115,934件

メールアドレス 127,838件

電話番号 67,662件

フリガナ 81,841件

3.原因

Webサイト及びモバイルアプリを表示するために、ユーザー情報を閲覧するAPIを提供しています。そのAPIは、本来はサイトに公開されている情報（ニックネームやアイコンなど）をユーザーIDを指定して閲覧するためのAPIですが、一部本人以外が閲覧できるべきではない項目が閲覧できるようになっていました。

4.対応状況

脆弱性に対する対応は全て完了しております。

5.TABICAユーザーの皆様へのお願い

TABICAからユーザーに対して個人情報を聞き出す、パスワード等の変更を要求するなどの個別連絡は一切致しません。TABICAになりすました連絡にはご対応されませんようご注意ください。

6.本件に関するお問い合わせ窓口

大変お手数をお掛けいたしますが、下記フォームよりご連絡いただきますようお願い申し上げます。

https://tabica.jp/entry/fixed/inquiry/
