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。

●教育サービスに不正アクセス…122万人分のアカウント情報閲覧か

https://www.nikkei.com/article/DGXMZO57989360T10C20A4CC1000/
https://www3.nhk.or.jp/news/html/20200413/k10012385261000.html
https://corp.classi.jp/news/1926/

このニュースをザックリ言うと･･･

- 4月13日(日本時間)、ベネッセホールディングスとソフトバンクの合弁会社Classi社より、同社が運営する中～高校向けクラウドサービス「Classi」が不正アクセスを受けたと発表されました。

- 不正アクセスは4月5日14時～16時に海外のIPアドレスから発生、ユーザー約122万人のIDとハッシュ化されたパスワード、任意記入の教員の公開用自己紹介文2,031件分(うち11件分は氏名・勤務先が特定可能な情報を含んでいた)が閲覧された可能性があるとのことです。

- 同社では6日にセキュリティ対策を行った上でサービスの再開を行っており、以後はベネッセグループの各サービス含め不正アクセスは確認されていないとしており、またユーザーに対しパスワードの変更を呼び掛けています。

AUS便りからの所感等

- ベネッセとしては、2014年に発覚した、最大3,504万件の個人情報が内部関係者によって持ち出された事件以来の大規模な情報流出となり、Classiアプリも全国の高校の約半数、高校生の1/3が利用しているとのことで影響範囲は広いとみられます。

- 前述の通りパスワードそのものは流出していませんが、パスワードのハッシュ化方法次第では、いわゆる「レインボーテーブル」を用いての高速な解読が行われる恐れが、さらには「リスト型攻撃」のターゲットとされる可能性も考えられます。

- 対象となるユーザーにとっては、当該サービスのパスワードの変更はもちろん、同じパスワードを他のサービスで使い回しているのであれば、そちらも(他と共有していない別のパスワードに)変更する必要があるでしょう。

日本経済新聞

122万人分IDに不正アクセス、教育サイト「クラッシー」

サービス・食品
2020/4/13 18:58

保存 共有 印刷 その他

ベネッセホールディングスとソフトバンクの共同出資会社Classi（クラッシー、東京・新宿）は13日、外部からの不正アクセスがあったと発表した。高校生ら約122万人分のIDや、暗号化されたパスワードの文字列などが閲覧された疑いがあるという。既に不正アクセスは遮断されたが、利用者に対してパスワードの変更を呼びかけている。

クラッシーはオンライン学習用の教材などを配信する教育機関向けのサービス。5日に予期しない事象が発生してサービスを停止し、調査したところ外部の攻撃により不正アクセスが確認されたという。

サービスを利用する生徒や保護者、教育機関のIDなどのほか、任意で記入された教師の自己紹介文2031件が閲覧された疑いがある。パスワード自体は閲覧されていないという。

6日にサービスを再開し、同日以降は不正アクセスは起きていない。必要な対応は完了したが、サイト上で利用者にパスワードを変更するように呼びかけている。

Classi

2020年4月13日
Classi株式会社

Classiご利用の皆様へ

サービス一時停止の調査報告とパスワード変更のお願い

平素より、Classiをご利用いただき誠にありがとうございます。
Classiの障害調査のため、ご利用いただけない期間をいただきましたが、調査の結果、外部からの不正アクセスがあったことが判明いたしましたので、ご報告させていただきます。ご迷惑ご心配をおかけし、誠に申し訳ございません。
この不正アクセスにより閲覧された可能性があるものは、お客様がご利用中のClassiを利用するためのID、暗号化されたパスワードの文字列（※パスワード自体は対象ではございません）と先生方の任意で記入いただいた自己紹介文となっております。
それ以外のお客様の情報については、不正アクセスされた対象には含まれておりません。詳細は下記をご参照ください。
また、既に不正アクセスは遮断されており、必要な対応は完了しておりますが、万全を期するために、皆様にパスワードの変更をお願いさせていただいております。
ご不便とお手数をおかけしますことを重ねてお詫び申し上げます。

記

1.第三者による不正アクセスの概要について
Classiは、2020年4月5日（日）夕刻に予期しない事象が発生し緊急でサービス停止をしておりました。これについて、不正アクセスの疑いを含めて調査を開始し、外部専門会社の協力を得て不審ファイルや通信ログを解析したところ、外部の攻撃者により不正アクセスが行われていたこと、および、この不正アクセスにより閲覧された可能性のある情報の範囲とその内容が、4月11日（土）に確定しました。
なお、4月6日（月）のサービス再開時点で、すでに必要な対応は完了しております。4月6日以降の不正アクセスはございません。

●台湾・米・独政府機関がZoomを使用しないよう勧告…セキュリティ懸念から

https://japan.cnet.com/article/35152112/
https://japan.cnet.com/article/35152254/
https://gigazine.net/news/20200409-google-bans-zoom/

このニュースをザックリ言うと・・・

- 4月7日(現地時間)、台湾の内閣より、Zoomや「セキュリティやプライバシーで懸念がある」その他のビデオソフトウェアを使用しないよう勧告が出されました。

- GoogleやMicrosoftが提供するソフトウェア(Google Meet、Skype、Teams等)を含む他の選択肢は引き続き許可され、代替として使用を検討すべきとしています。

- 米上院やドイツ外務省等の各国政府機関、あるいはGoogleにおいても従業員に対し、使用の禁止が通達されているとのことです。

AUS便りからの所感

- Zoomについてはテレワーク用途での利用が拡大したのとともにセキュリティ上の各種問題が指摘されている(「AUS便り 2020/4/6号」参照)他、いわゆる「リスト型攻撃」により奪取されたとみられる、50万人分以上のアカウント情報が攻撃者の間で売買されているとのニュースもあります(https://gigazine.net/news/20200414-hacker-sold-over-500k-zoom-accounts/)。

- Zoom側では引き続き各種セキュリティ対応の改修を行っている模様ですが、利用者側としては安全性の検討を十分に行い、最低でもパスワードの設定等現時点で提供されているセキュリティ機能を確実に使用することが肝要であり、また特定のサービスに依存せず、場合によっては他のサービスに随時移行できる等の体制も整えておくべきでしょう。

●「Google Chrome 81」「Microsoft Edge 81」に重大な脆弱性、アップデートの確認を

https://forest.watch.impress.co.jp/docs/news/1247428.html
https://forest.watch.impress.co.jp/docs/news/1248104.html

このニュースをザックリ言うと・・・

- 4月15日(現地時間)、Googleより、同社開発のWebブラウザー「Chrome」に脆弱性1件(CVE-2020-6457)が確認されたとして、修正バージョン「81.0.4044.113」がリリースされています。

- 脆弱性はChromeの音声認識機能に存在し、同社基準での危険度は最も高いレベルに指定されているとのことです。

- 同17日にはMicrosoftからも、Chromeと同じエンジンを使用している「Microsoft Edge 81」について修正バージョン「81.0.416.58」がリリースされています(Chromeベースではない古いバージョンは脆弱性の影響を受けないとみられます)。

AUS便りからの所感

- Chrome 81は4月7日に、Edge 81も同じく同13日に安定版として初めてリリースされたばかりでした。

- Chromeは通常の設定で自動更新が行われますが、タイミング上前述のバージョンにまだ更新されていない可能性もあるため、ブラウザーを起動した際に念のためバージョン情報を確認することを推奨致します(Chromeの場合は「右上のアイコン→ヘルプ→Google Chromeについて」で確認可能、最新でなければ更新が開始されます)。

- また、ブラウザー側で脆弱性の対応が行われる前に攻撃を受ける可能性もあるため、アンチウイルスやUTMによる防御も別途万全に行うことが重要です。