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。

●「mineo」運営会社、約6500件のIDで不正ログイン…パスワードリスト型攻撃と判明

https://japan.cnet.com/article/35124164/
http://www.k-opti.com/press/2018/press38.html

このニュースをザックリ言うと・・・

- 8月16日（日本時間）、MVNO※サービス「mineo(マイネオ)」や光通信サービス「eo」等を提供するケイ・オプティコム社より、同社ユーザ向けアカウント「eoID」が外部より不正ログインの被害を受けたと発表されました。
※MVNO（Mobile Virtual Network Operator、仮想移動体通信事業者）

- 発表によれば、8月13日22時5分～8月15日21時0分の間に計6458件のeoIDが不正ログインされ、住所・氏名・性別・電話番号・生年月日・メールアドレス等が閲覧された可能性があるとされています（口座情報・クレジットカード情報については、マスキング処理を施されており流出の可能性はないとのことです）。

- 同社サーバから直接アカウント情報が流出したのではなく、他のサービスから流出したアカウント情報を悪用した、いわゆる「パスワードリスト型攻撃」が行われたものとされており、該当する各ユーザに対してはパスワードを変更するまでeoIDが利用できないよう対策をとったことを個別に連絡しているとのことです。

AUS便りからの所感等

- 8月14日にNTTドコモのアカウントが不正ログインを受けたことが発表されており、やはりリスト型攻撃であったことが明らかになっています（「AUS便り 2018/08/20号」参照）。

- 残念ながら現時点でeoIDに2段階認証の設定はできない模様ですので、他のサービスと共通でない、十分に強力なパスワードを設定することが必須となります。

- ただし、今回被害を受けていなくても、あるいは2段階認証が設定できるサービスであっても、今回の事件を対岸の火事と思わず、強力なパスワードを設定しておくことを常に念頭に置いておくことが重要です。


cnet Japan

「mineo」運営会社、約6500件のIDで不正ログイン--パスワードリスト型攻撃と判明

山川晶之 （編集部） 2018年08月16日 20時48分

ケイ・オプティコムは8月16日、同社が展開する光通信サービス「eo」や格安モバイル通信サービス「mineo」などを利用するための「eoID」に対し、外部からの不正ログインがあったと発表した。現時点では、顧客データの流出は確認できていないとしている。

お知らせ　印刷用ページを表示

同社では、特定のIPアドレスからeoIDへの不正ログインを試みる事象を確認し、このIPアドレスからのログインを遮断する緊急措置を実施。不正ログイン発生期間は、8月13日22時5分から8月15日21時までという。調査の結果、ケイ・オプティコムへのハッキングによるeoIDの流出ではなく、第三者がユーザーIDやパスワードを不正に入手してログインを試みる「パスワードリスト攻撃」によるものと判明したという。

不正ログインが確認されたユーザー数は、8月15日21時時点で6458件。閲覧された可能性のある情報は、住所、氏名、性別、電話番号、生年月日、メールアドレスなどで、口座情報やクレジットカード情報については、マスキング処理を施していたことから流出の可能性はないという。

8月15日よりeoIDへの不正ログインが確認されたIDに関しては、パスワードを変更なしに利用できないように対策済であり、該当ユーザーには個別メールで連絡しているという。同社では、不正ログイン防止として、他社サービスとは違う、第三者が容易に推測できないようなパスワードにするよう注意喚起している。


K-OPTI.COM

お知らせ　印刷用ページを表示

eoIDに対する不正なログインについて

2018年8月16日
株式会社ケイ・オプティコム

株式会社ケイ・オプティコム(以下ケイ・オプティコム、代表取締役社長:荒木 誠／本社:大阪市中央区)が提供するeoやmineoなどの各種をご利用いただくためのeoIDに対し、外部からの不正なログインがあったことが判明いたしました。弊社の顧客データが流出した事実は、現在確認できておりませんが、お客さまにはご迷惑とご心配をおかけいたしますことを深くお詫び申し上げます。

1.経緯
昨日(8月15日

2.不正ログインの状況
不正ログインが確認されたユーザー数 … 6,458件(2018年8月15日21時現在)
閲覧された可能性のある情報 … お客さまの住所、氏名、性別、電話番号、生年月日、メールアドレスなど
*口座情報、クレジットカード情報についてはマスキングをしており、流出した可能性はありません。

3.対応状況
昨日(8月15日)よりeoIDへの不正ログインが確認されたIDに関しては、パスワードを変更しなければ利用できないように対策を講じており、該当のお客さまには個別メールにてご連絡させていただいております。

4.お客さまへのお願い
eoIDをご利用のお客さまは、不正ログインを防止するために以下の点にご注意ください。
(1)他社サービスとは違うパスワードを設定する。
(2)第三者が容易に推測できるパスワードを使用しない。

弊社といたしましては、今回の事態を厳粛に受け止め、セキュリティーの強化に取り組んでまいります。

●ポートスキャンで不必要な公開を把握すべき…NRIセキュア調査

https://japan.zdnet.com/article/35124332/

このニュースをザックリ言うと・・・

- 8月21日（日本時間）、NRIセキュアテクノロジーズ社より、2017年度に同社のセキュリティ対策サービスを利用する法人のセキュリティ状況を調査、分析した「サイバーセキュリティ傾向分析レポート 2018」が発表されました。

- 発表によれば、同社ファイアウォール製品がブロックした通信のうちIoT関連とみられるサービスへの通信が38.0%にのぼり、特に29.2%がtelnetサービスポートに対するものだったとされています。

- また、Webサイト約13万サイトのうち12.2%について、不必要なサービスポートの他、「manage.example.com」といった管理用サブドメイン、あるいは「www.example.com/admin」といった管理ページへの外部からのアクセスが可能だったとしています。

- こういった結果をもとに、同社では「ポートスキャン等によって不要な外部開放が行われていないか、いま一度現状把握から着手して頂きたい」と結論付けています。

AUS便りからの所感等

- 今日においては、サービスポートのみならずWebサイトの管理用ページ等も含めた、攻撃者が容易に推測し得る場所は、ポートスキャナあるいはWeb系のスキャナによって検出される可能性が非常に高く、フリーのソフトウェアでも比較的精度の高いものが多く存在します。

- 逆に言えば、そういったツールを攻撃者が使ってくる前に自分たちで使用する、あるいは攻撃者ではない第三者からの診断を受けることがセキュリティを固めるために重要なことと言えます。


ZDNet Japan

ポートスキャンで不必要な公開を把握すべき--NRIセキュア調査

NRIセキュアテクノロジーズは8月21日、「サイバーセキュリティ傾向分析レポート 2018」を発表した。IoTマルウェアの侵入などにつながるインターネットへの不必要なポートの公開に警鐘を鳴らしている。

調査は2005年度から毎年実施しているもので15回目となる。2017年度に同社のセキュリティ対策サービスを利用する法人でのセキュリティ状況を調査、分析している。

- こうしたセキュリティ診断等を受け、防御を固めるべき場所を把握した上で、不要なポートを閉じる、アクセス制限を行う、それらができない場合はポート番号やアクセスする場所の名前を安易に推測しにくいものに変更する、そしてそれを探り出そうとするアクセスをIDS・IPS等で遮断するといった対策を検討することが肝要です。

●「Apache Struts2」の脆弱性を悪用した攻撃コードが出回る、早急に修正版へのアップデートを

https://internet.watch.impress.co.jp/docs/news/1139364.html

このニュースをザックリ言うと・・・

- 8月24日（日本時間）、IPAやJPCERT/CCより、Webアプリケーションフレームワーク「Apache Struts2」にリモートから任意のコードが実行可能な脆弱性（S2-057）が含まれているとして警告が出されています。

- 警告によれば、Struts2を使用しているWebサーバに対し外部から不正なリクエストを送信することにより、サーバを乗っ取られる可能性もあるとされており、既に脆弱性を突く攻撃コードが出回っているとのことです。

- 脆弱性が修正されたバージョン2.3.35、2.5.17がリリースされており、これらより前のバージョンを使用している場合はアップデートすることが推奨されている他、回避策も示されています。

AUS便りからの所感等

- Struts2は大規模なWebサイトで頻繁に利用されている一方で、今回のような重大な脆弱性の発見がたびたび話題となっており、脆弱性を修正していないWebサーバへの攻撃による個人情報等の流出も多く発生しており、例えば、クレジットカード情報の入力フォームが改ざんされるケースもありました。

- WAF（Webアプリケーションファイアウォール）等の設置により、脆弱性を突く不正なリクエストのパターンを遮断することが期待されますが、アンチウイルスと同様、どれだけ速やかに対応してくれるか、またパターンファイル等をどれだけ早く更新するかが肝となるほか、根本的な対策として、前述の通りアップデートや回避策の適用は忘れずに行うべきです。


INTERNET Watch

「Apache Struts 2」の脆弱性を悪用した攻撃コードが出回る、早急に修正版へのアップデートを

磯谷 智仁　2018年8月23日 14:49

JPCERT/CCによると、同脆弱性はApache Struts 2の処理に起因しており、Strutsの設定ファイル（struts.xmlなど）でnamespaceの値が指定されていないか、ワイルドカードが指定されている場合、あるいは、URLタグの記述において“value”か“action”の値が指定されていない場合に影響を受けるとしている。

問題　ソフトウェアフレームワーク「Apache Struts 2」には、リモートから任意のコード実行可能な脆弱性が存在します。

① 攻撃者が、「Apache Struts 2」に悪意あるリクエストを送信する

悪意あるリクエスト　攻撃者　② 任意のコードが実行されてしまう　「Apache Struts 2」が設置されたサーバ

「Apache Struts 2」における任意のコードが実行可能な脆弱性のイメージ（IPAによる注意喚起より）