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。

●大手ネット証券、フィッシングによるユーザーアカウント奪取、不正取引相次ぐ…マルウェアによる可能性も指摘

https://www3.nhk.or.jp/news/html/20250321/k10014756511000.html
https://www.itmedia.co.jp/news/articles/2503/24/news180.html
https://www.rakuten-sec.co.jp/web/info/info20250325-01.html

このニュースをザックリ言うと･･･

- 3月21日(日本時間)、大手ネット証券の楽天証券より、フィッシング詐欺によるとみられる同証券ユーザーのアカウント奪取、ないし不正な取引が発生しているとして注意喚起が出されています。

- 発表および各種報道によれば、被害は2024年12月頃から発生しており、金融商品の売却や中国関連株の購入が勝手に行われる等が報告されている模様です。

- 楽天証券では、同23日に通常と異なる端末からのログインに対する追加認証(リスクベース認証)の提供を開始(他の多要素認証等も以前から提供されています)、同25日までに中国株(計582銘柄)の買い注文を一時停止する等の対応を行っており、他のネット証券各社も相次いで注意喚起や新たな認証機能提供等の対応を行っています。

- 一方で、フィッシングメール等を受け取っていないのに被害を受けたとするユーザーの報告もあり、オンラインバンキング等のアカウント情報を抜き取るマルウェア(インフォスティーラー)に感染した可能性も指摘されています。

AUS便りからの所感等

- フィッシングメールは、日本データ通信協会の迷惑メール相談センター(https://www.dekyo.or.jp/soudan/contents/news/alert.html)において、「【重要】オンラインサービスご利用条件の変更について（要確認）」「【楽天証券】アカウント保護のための最新情報」等の件名による事例が複数掲載されている他、ショートメールによるもの等も報告されています。

- NHKの報道においては送信元メールアドレスに「@shiga .jp」「@kagoshima .jp」といったドメイン名を使用している事例が挙げられていますが、必ずしも全てがそうとは限らず、例えば楽天証券自体の「@rakuten-sec.co.jp」を使用しているものもあることに注意してください。

- 利用しているネット証券やその他金融機関サービスにおいて、スマートフォンでの生体認証等によるアカウントを保護する機能が提供されていないか確認し、速やかに設定を行うことを推奨致します。

- 併せて設定されているパスワードが推測されやすかったり他のサービスと共有していたりしないかも確認し、必要に応じより強固なパスワードに変更すること、もちろんインフォスティーラーを含めたマルウェアへの感染を抑制するため、アンチウイルスやUTMによる防御等を図ることも重要です。

NHK

楽天証券 偽メールで個人情報抜き取り被害 相次ぐ 注意呼びかけ

2025年3月21日 17時19分

ネット証券大手の楽天証券は、顧客の間で会社が送信したように装ったメールから偽のサイトに誘導され、個人IDなどのアカウント情報を抜き取られる被害が相次いでいると公表しました。身に覚えのない株式の売買が行われたと訴える顧客もいて、会社は不審なメールは削除するなど、注意を呼びかけています。

楽天証券によりますと、「口座の安全の確認の必要がある」などと会社が送信したように装ったメールが顧客宛てに送信され、偽のサイトに誘導されたあとIDやパスワードなどのアカウント情報が盗み取られるという被害が去年12月ごろから増えているということです。

● PHPに6件の脆弱性、セキュリティアップデートリリース

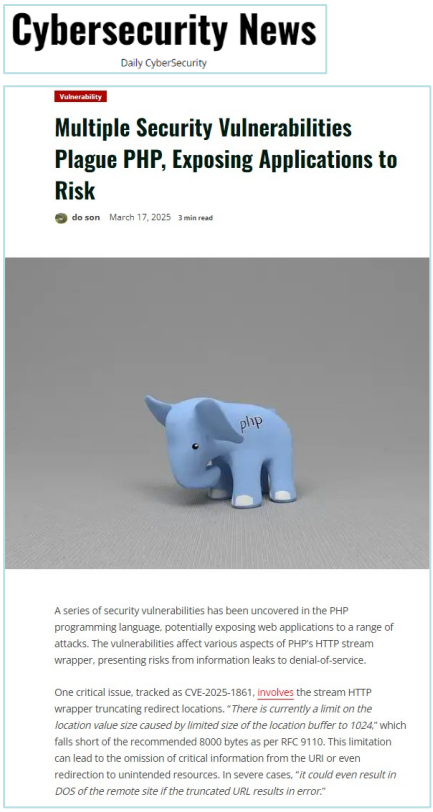
https://news.mynavi.jp/techplus/article/20250321-3158218/
https://securityonline.info/multiple-security-vulnerabilities-plague-php-exposing-applications-to-risk/

このニュースをザックリ言うと･･･

- 3月13日(現地時間)、プログラミング言語「PHP」の最新バージョン8.4.5, 8.3.19, 8.2.8, 8.1.32がリリースされています。
- 同17日のCybersecurity Newsではこれらのバージョンで修正された5件の脆弱性(CVE-2025-1861, CVE-2025-1734, CVE-2025-1217, CVE-2025-1219, CVE-2025-1736)について言及しており、サービス拒否や予期しない結果を引き起こす可能性があるとしています。
- この他8.4.5, 8.3.19ではさらに1件の脆弱性(CVE-2024-11235)が修正されています。

AUS便りからの所感

- PHPのアップデートは不定期に行われますが、セキュリティアップデートと銘打ったものとしては2024年11月以来となります。
- PHPは多岐にわたる機能・モジュールが本体に含まれており、例えば脆弱性が存在する機能やモジュールを使用・有効にしている次第でアップデート実施の可否を判断することも考えられますが、特に構築しているWebサイトが大規模になる程、Web経由で脆弱性を突かれる可能性が高くなるため、計画的かつ速やかにアップデートを行うことを推奨致します。


Cybersecurity News
Daily CyberSecurity

Vulnerability

Multiple Security Vulnerabilities Plague PHP, Exposing Applications to Risk

do son March 17, 2025 3 min read

A series of security vulnerabilities has been uncovered in the PHP programming language, potentially exposing web applications to a range of attacks. The vulnerabilities affect various aspects of PHP's HTTP stream wrapper, presenting risks from information leaks to denial-of-service.

One critical issue, tracked as CVE-2025-1861, involves the stream HTTP wrapper truncating redirect locations. *"There is currently a limit on the location value size caused by limited size of the location buffer to 1024,"* which falls short of the recommended 8000 bytes as per RFC 9110. This limitation can lead to the omission of critical information from the URI or even redirection to unintended resources. In severe cases, *"it could even result in DOS of the remote site if the truncated URL results in error."*

●アプリ登録完了メール送信で「To: 」にメールアドレス記載、8989件のアドレス流出か

https://www.itmedia.co.jp/news/articles/2503/19/news190.html
https://www.mcdonalds.co.jp/company/info/250318a/

このニュースをザックリ言うと･･･

- 3月19日(日本時間)、日本マクドナルドホールディングス社より、「マクドナルド公式アプリ」登録者へ送信されたメールにおいて、メールアドレスが他の登録者から閲覧可能な状態となっていたと発表されました。
- 当該アプリへ3月12日～13日に登録したユーザーに対し、同14日に登録完了メールを送信した際、1通につき最大500件分のメールアドレスを誤って「To(送信先)」欄に記載していたのが原因としています。
- 影響を受けたメールアドレスは8989件とされています。

AUS便りからの所感

- 同社では再発防止策として「メール配信システムの見直し、ならびに配信時の確認作業の厳重化」を行うとしています。
- メーラーからBcc: 欄に手動で多数の宛先を入力する形での送信をしていたとみられ、この方法はしばしばTo: 欄に誤って入力したことによるメールアドレス漏洩事案が報告されています。
- 一般にそういったケースでは「同報メール配信システム・メーリングリスト等を活用する」「メーラーで対応せざるを得ない場合はメーラー自身やアドオンの誤送信防止機能を使用する」「メールサーバーやUTMにおいて不審な大量送信時のチェック機構等を採用する」等、システム側での対策を行うことを検討し、また大量送信を想定したテスト等も事前に十分に実施することが望ましいです。

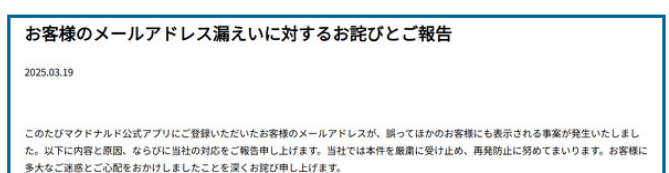
ITmedia NEWS

登録完了メールでメアド漏えい　マクドナルドアプリ、「To」欄に他ユーザーのメアド誤記載

2025年03月19日 17時15分 公開　[ITmedia]

日本マクドナルドホールディングスは3月19日、マクドナルド公式アプリに登録した顧客に登録完了メールを送る際、誤って「To」欄に他の顧客のメールアドレスを記載する設定で配信してしまい、顧客のメアドが漏えいしたと発表した。

誤記載されたアドレスは1通につき最大500件ずつ。影響を受けたアドレスの総計は8989件という。


お客様のメールアドレス漏えいに対するお詫びとご報告

2025.03.19

このたびマクドナルド公式アプリにご登録いただいたお客様のメールアドレスが、誤ってほかのお客様にも表示される事案が発生いたしました。以下に内容と原因、ならびに当社の対応をご報告申し上げます。当社では本件を厳重に受け止め、再発防止に努めてまいります。お客様に多大なご迷惑とご心配をおかけしましたことを深くお詫び申し上げます。