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。

●漫画出版社のWebサイト改ざん、不正なメールフォーム設置…フィッシングメール送信に悪用か

https://scan.netsecurity.ne.jp/article/2023/10/16/50089.html
https://www.akitashoten.co.jp/news/2921

このニュースをザックリ言うと･･･

- 10月5日(日本時間)、大手漫画出版社の秋田書店より、同社Webサイトが不正アクセスを受け、改ざんの被害を受けていたと発表されました。

- 発表によれば、改ざんにより、不正なメールフォームが設置されていたことが確認されており、フィッシング詐欺メールに利用されていた可能性があるとのことです。

- 被害を受けたサーバーで運用していたWebサイトは閉鎖済みであり、また個人情報に関するデータも取り扱っておらず、個人情報の流出はないとしています。

AUS便りからの所感等

- メールフォームは、外部からの問合せ受け付け用のソフトウェアが設置され、「問合せた内容を入力者に送り返す」メールを第三者に送信する形でフィッシングメールの拡散を行ったと推測されます。

- これによって送信されたメールが相手側で不正なメールと判定されるかはサーバー構成やSPF・DMARC等の設定次第であり、Webサーバーが外部とのメールのやりとりを行うメールサーバーを兼ねている場合や、Webサーバーから無条件で(SMTP認証なしで)そのようなメールサーバーを利用可能な設定の場合、フィッシングメールが正当なものと認識されてしまう可能性が高くなることを留意すべきでしょう。

- このようなサーバーへの侵入は例えば組織内ネットワークへの侵入の足掛かりとなる恐れもあるため、サーバーやWebアプリケーションの管理アカウントについては強固なパスワードの設定等厳密な管理を行うこと、また管理者のPCにもマルウェアが感染する等して、そのような管理アカウントへの不正ログインが発生することがないよう、アンチウイルスやUTM等による防御も肝要です。

ScanNetSecurity by iid

2023.10.16 Mon 8:05

秋田書店のWebサーバに不正アクセス、フィッシング詐欺メールに利用された可能性

株式会社秋田書店は10月5日、同社Webサーバへの不正アクセスについて発表した。

シェア　ポスト　送る

株式会社秋田書店は10月5日、同社Webサーバへの不正アクセスについて発表した。

これは同社が管理運用するWebサーバに第三者からの不正アクセスがあり、不正なメールフォームが設置されていたというもの。同社では既に、当該Webサーバで運用していたWebサイトは閉鎖しているが、フィッシング詐欺メールに利用されていた可能性があることを確認しているという。

トップページ

全２枚

拡大写真

●cURLに「過去最悪」のもの含む脆弱性2件報告、バージョン8.4.0リリース

https://news.mynavi.jp/techplus/article/20231011-2790377/
https://curl.se/docs/CVE-2023-38545.html
https://curl.se/docs/CVE-2023-38546.html
https://sysdig.jp/blog/cve-2023-38545/

このニュースをザックリ言うと・・・

- 10月11日(現地時間)、オープンソースのマルチプロトコルクライアントおよびライブラリである「cURL」の開発元より、cURLに2件の脆弱性が報告され、修正バージョン8.4.0がリリースされています。

- 脆弱性のうちSOCKS5プロキシー使用時におけるヒープオーバーフローの問題(CVE-2023-38545)は非常に危険度が高いものとされ、Linuxディストリビューションのパッケージでも RHEL 9(およびAlmaLinux 9/Rocky Linux 9)等で修正バージョンがリリース済み(RHEL 8以前等は影響なし)です。

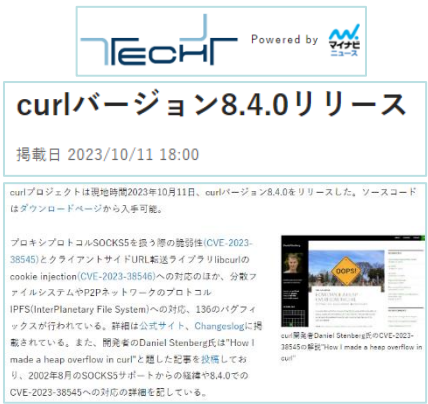
- 一方不正なCookieの挿入の問題(CVE-2023-38546)は比較的危険度は低いとされ、RHEL系では8以前にも影響するとみられますが、修正バージョンがリリースされているのは現在9系のみとなっています。

AUS便りからの所感

- cURLはサーバーから別のサーバー上のファイルをダウンロードする等の目的で多数のソフトウェアから利用されることがあり、リモートから直接脆弱性を悪用されるよりも、不正なWebサーバーへ接続するよう誘導する等の受動的攻撃が行われる可能性が考えられます。

- 脆弱性の存在・修正バージョンのリリースは10月3日に予告されており、特にCVE-2023-38545についてはcURLにおける過去最悪の脆弱性とされ、詳細はバージョン8.4.0のリリースまで明かされなかった一方、実際の攻撃には非常に長いホスト名を持つサーバーへ誘導する必要があり、悪用はそう簡単なものではないとする意見もあります。

- ともあれ、外部に公開されたサーバーに直接影響するものだけでなく、OS自体から各種アプリケーション・ライブラリーまで全て最新バージョンに保つよう、Linuxであればyum(dnf)・aptによるパッケージの随時更新を実行することが重要です。



●ETC利用照会サービスへの不正ログイン発生、高速道路6社より発表

https://scan.netsecurity.ne.jp/article/2023/10/16/50088.html
https://www.etc-meisai.jp/news/231004.html
https://xtech.nikkei.com/atcl/nxt/column/18/00598/100500236/

このニュースをザックリ言うと・・・

- 10月4日(日本時間)、国内の高速道路を運営する6社(NEXCO東日本・NEXCO中日本・NEXCO西日本・首都高速道路・阪神高速道路・本州四国連絡高速道路。以下・各社)より、各社で運営される「ETC利用照会サービス」において不正ログインの被害が発生していたと発表されました。

- 不正ログインは9月30日～10月2日に海外から行われ、一部顧客の個人情報(メールアドレス・登録ID・秘密の質問・答え・利用履歴)を閲覧された可能性があるとされています。

- 各社では被害を受けたユーザーに個別に連絡をとり、今後大量アクセスがあったIPアドレスのブロックを行うとしています。

AUS便りからの所感

- 発表では明言されていないものの、度々話題となる「リスト(パスワードリスト)型攻撃」の一環とみられますが、セキュリティ研究者のpiyokango氏は、ETC利用照会サービスのユーザーIDは「半角の英数字記号を4～12文字組み合わせたもの」であり、メールアドレスのローカルパート(@より前の部分)とパスワードの組み合わせによる攻撃が行われた(該当するユーザーがターゲットとなった)可能性があると推測しています。

- ユーザー側においてはこれまでも注意喚起されている通り、サービス毎に異なる推測されにくいパスワードを設定することが重要で、加えて今回のようにIDも設定可能な場合はメールアドレスのローカルパートと同一のIDを避けることも検討に値するでしょうが、一方であるパスワードから少々の変更を行った程度のパスワードを比較的高い精度で推測する手法(AUS便り 2023/10/04号)がIDの推測にも用いられることも考えられ、少なくともパスワードは可能な限りランダムなものを設定することを心掛けるべきでしょう。