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。

●PixelスマートフォンとWindows、スクリーンショット機能の脆弱性報告…切り取り＆黒塗り箇所復元の可能性

https://www.techno-edge.net/article/2023/03/20/1040.html
https://www.techno-edge.net/article/2023/03/22/1048.html
https://twitter.com/ItsSimonTime/status/1636857478263750656

このニュースをザックリ言うと･･･

- 3月18日(日本時間)、海外のエンジニアにより、Google製Pixelスマートフォンのスクリーンショット編集機能「Markup」に脆弱性「aCropalypse(CVE-2023-21036)」が存在すると発表されました。

- 脆弱性はMarkupによるスクリーンショット画像の切り抜きやマスク処理の際に発生するもので、画像ファイルから切り抜き・マスクされた箇所を復元される可能性があるとされています。

- 同22日には、同じ機能をもつWindows 10に附属する「切り取り＆スケッチ」および11に附属する「Snipping Tool」においても同様の脆弱性(CVE-2023-28303)の存在が報告されています。

- Pixelにおいては3月6日リリースのセキュリティアップデートで、Windowsにおいても3月24日リリースの「切り取り＆スケッチ」バージョン10.2008.3001.0および「Snipping Tool」バージョン11.2302.20.0において脆弱性が修正されているとのことです。

AUS便りからの所感等

- 脆弱性は、画像の修正時に本来ファイルサイズが削減されるところで、サイズの切り詰め処理を行わないために、修正前のデータが一部残ってしまうことが原因とされています。

- Androidやツールのアップデートおよび安全なバージョンかの確認の他、過去にそれらを用いて作成した画像をWebにアップロードしたり、Word等Office文書やPDFに貼り付けて公開していた場合に情報を復元される恐れがあるとされ、可能な限り差し替えを行うことも推奨されています(PNG画像を他のツールで加工したり、JPEG画像等に変換した場合は問題はないとされます)。

- 今回の脆弱性はソフトウェア上の問題に起因したものですが、例えばOffice文書において黒く塗りつぶした図形を文章・画像の上からかぶせるマスク処理では、マスクの下に隠れた部分を容易に読み取られてしまうため、隠れた文字部分も適切に削除する等に注意すること、またPDF文書についても同様の問題に対応する有償・無償のツールが提供されているので利用することが重要です。

TECHNO EDGE

Google Pixelのスクショ編集で消した部分が復元される脆弱性「aCropalypse」、塗り潰しや切り取り範囲外を復活

Ittousai

Google Pixelスマートフォンのスクリーンショット編集機能「Markup」に、編集前の画像を漏洩する脆弱性があることが分かりました。

たとえばPixel でメールやメッセージなどのスクリーンショットを撮影して、見せたくない分を切り取ったり、塗りつぶして隠したつもりでも、ネットにアップロードした画像ファイルからクロップアウトしたはずの部分や、塗りつぶしたはずの部分を読み取られる可能性があります。

Windows 11にもスクショで情報漏洩の脆弱性、切り取り範囲外や消した部分が復元できる可能性

Ittousai

Androidで見つかったスクリーンショット編集機能の脆弱性が、Windows 11の純正スクリーンショットツールにもあることが分かりました。

Windows 11 / 10標準のSnipping Tool (Win+Shift+S)でスクリーンショットを撮影してから、切り取ったりマークアップで塗り潰して上書き保存した場合、切り取った範囲外や消したはずの部分がファイルに含まれる場合があります。

●大阪急性期・総合医療センターのランサムウェア感染に関する報告書公開…ホスト間でパスワード共有等の問題

https://www.itmedia.co.jp/news/articles/2303/28/news179.html
https://www.gh.opho.jp/important/785.html

このニュースをザックリ言うと･･･

- 3月28日(日本時間)、大阪急性期・総合医療センターより、2022年10月31日に同センターで発生(AUS便り 2022/11/15号参照)したサイバー攻撃に関する調査報告書が公開されました。

- 同センターの電子カルテシステムがランサムウェア感染等の被害を受け、復旧まで約2ヶ月かかる等の事態となっています。

- (当時も報じられていましたが)まず同センターから患者給食業務を委託されていた業者のシステムが侵入されており、ここから閉域網を経由して同センターが不正アクセスを受けたことが報告書で明らかになっています。

- また今回、同センター内のシステムにおいても、「電子カルテサーバーにアンチウイルスソフトが導入されていなかった」「Windowsのパスワードがサーバー・端末毎に全て共通」等、運用上の問題が多く存在していたことが指摘されています。

AUS便りからの所感

- 他に指摘されていた問題点として「アカウントロック設定がなかった」「ユーザー全てに管理者権限を与えていたため、攻撃者にアンチウイルスソフトをアンインストールされた」等があり、これらが原因で各サーバー間への「横展開」を許す結果となっています。

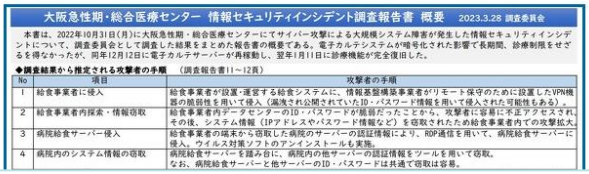
- 攻撃の舞台となったのは大規模な医療機関とはいえ、直接的な攻撃ではなく、内部ネットワークと相互に接続されている別の拠点あるいは組織のネットワークから攻撃を受ける可能性はどの組織でも決してあり得ないものではなく、調査報告書に記載されている原因と対策を既に実行しているか否かに拘わらず確認し直し、全ての端末・サーバーへのアンチウイルスの導入・有効化はもちろん、一般ユーザーから管理者までのアカウント運用状態の点検、適宜UTM等を用いてのネットワークの分割等、とり得るべき各種対策を計画的に実行していくことが肝要です。

ITmedia NEWS

全員に管理者権限、パスワードは全部共通、脆弱性は放置…… ランサム攻撃受けた大阪急性期・総合医療センターのずさんな体制

2023年03月28日 19時50分 公開 [ITmedia]

2022年10月末にサイバー攻撃を受けたことで話題になった大阪急性期・総合医療センターが3月28日に、同件の調査報告書を公開した。調査によると、同センターではユーザー全てに管理者権限を付与していた他、数あるサーバやPCなどで共通のIDとパスワードを使用しており、侵入経路となったVPN機器は脆弱性が放置されているなどずさんな管理体制だったことが分かった。


大阪急性期・総合医療センター 情報セキュリティインシデント調査報告書 概要 2023.3.28 調査委員会

本書は、2022年10月31日(月)に大阪急性期・総合医療センターにてサイバー攻撃による大規模システム障害が発生した情報セキュリティインシデントについて、調査委員会として調査した結果をまとめた報告書の概要である。電子カルテシステムが暗号化された影響で長期間、診療制限をせざるを得なかったが、同年12月12日に電子カルテサーバーが再稼動し、翌年1月11日に診療機能が完全復旧した。

◆調査結果から推定される攻撃者の手順 (調査報告書Ⅰ～Ⅻ頁)

No	項目	攻撃者の手順
1	給食事業者に侵入	給食事業者が設置・運営する給食システムに、情報基盤構築事業者がリモート保守のために設置したVPN機器の脆弱性を用いて侵入(漏洩されぶ開されていたID・パスワード情報を用いて侵入された可能性もある)。
2	給食事業者内探索・情報窃取	給食事業者内データセンターのID・パスワードが脆弱だったことから、攻撃者に容易に不正アクセスされ、その後、システム情報(IPアドレスやパスワード情報など)を窃取されたため給食事業者内での攻撃拡大
3	病院給食サーバー侵入	給食事業者の端末から窃取した病院のサーバーの認証情報により、RDP通信を用いて、病院給食サーバーに侵入。ウイルス対策ソフトのアンインストールも実施。
4	病院内のシステム情報の窃取	病院給食サーバーを踏み台に、病院内の他サーバーの認証情報をツールを用いて窃取。 なお、病院給食サーバーと他サーバーのID・パスワードは共通で窃取は容易。

●家庭用ルーターのVPN・DDNS・外部からの管理画面アクセス設定に注意…警視庁より呼び掛け

https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/router.html

このニュースをザックリ言うと･･･

- 3月28日(日本時間)、警視庁より、家庭用ルーターがサイバー攻撃に悪用される可能性に対し注意喚起が出されています。

- 従来の対策、例えば「初期設定の単純なIDやパスワードは変更する」「常に最新のファームウェアを使用する」「サポートが終了したルーターは買い替えを検討する」のみでは対応できないケースがあるとし、メーカーと協力しての今回の注意喚起となったとしています。

- 今回新たなポイントとして、「見覚えのない設定変更がなされていないか」、例えば「VPN機能設定」「DDNS機能設定」あるいは「インターネット(外部)からルーターの管理画面への接続設定」が有効になっていないかの確認を呼び掛けています。

AUS便りからの所感

- 警視庁では上記のような設定変更の有無を「定期的に確認する」よう呼び掛けており、今後メーカー各社からも確認してほしい箇所の解説情報が提供されるとみられるため、利用しているルーターのベンダーサイトの確認を行うことを推奨致します。

- 一方、企業向けルーターでの設定内容をテキストファイルに出力する等の機能が一般の家庭用ルーターには実装されておらず、家庭のネット利用者や、企業で家庭用ルーターを使用するケースでこのような設定の確認はかなりの手間となることが指摘されています。

- 警視庁で着目しているサイバー攻撃の詳細な情報の提供、また家庭用ルーターにおける設定の確認を容易に行うツール等の提供が今後メーカーから行われるか等が注目されます。

警視庁

更新日：2023年3月28日

家庭用ルーターの不正利用に関する注意喚起

サイバー攻撃事案の捜査の過程で、家庭用ルーター（以下「ルーター」といいます。）が、サイバー攻撃に悪用され、従来の対策のみでは対応できないことが判明しました。警察では、複数の関係メーカーと協力し、官民一体となって注意喚起いたします。

使用された手法

今回確認された手法は、一般家庭で利用されているルーターを、サイバー攻撃者が外部から不正に操作して搭載機能を有効化するもので、一度設定を変更されると従来の対策のみでは不正な状態は解消されず、永続的に不正利用可能な状態となってしまう手法です。