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。

●偽のセキュリティソフトをインストールさせようとするフィッシング… ドコモが注意喚起

https://www.docomo.ne.jp/info/notice/pages/220826_00.html
https://www.docomo.ne.jp/info/anti-phishing/measure/delete_app/
https://k-tai.watch.impress.co.jp/docs/news/1435235.html

このニュースをザックリ言うと･･･

- 8月26日(日本時間)、NTTドコモより、セキュリティソフトを装った不審なアプリをインストールさせようとするフィッシングに注意喚起が出されています。
- 例として「お客様の端末から異常ログイン」「必ずセキュリティソフトをアップデート」「お客様の端末からウィルスが検出」といった文面のSMSが送られ、記載されたURLで「スマホ安心セキュリティ」等という名前のアプリのインストールや、ネットワーク暗証番号の入力を促すものが挙げられています。
- インストールにより、意図しない決済が発生した事案も確認されたとのことで、同社では注意を呼び掛けるとともに、不正なアプリを削除する方法を示しています。

AUS便りからの所感等

- ドコモが提供する「あんしんセキュリティ」アプリの偽物とみられており、2021年にもドコモから同様の注意喚起が出されています(https://www.docomo.ne.jp/info/notice/pages/210611_00.html)。
- SMS上のリンクからアプリをインストールするよう誘導されるケースは十中八九マルウェア感染等を意図したものであると認識し、安易なインストールを行わないこと、またアプリストアからインストールするケースも含め、デバイス上の権限の利用が不自然に要求された場合にもその場で許可せず、アプリストアやソーシャルネット等での評価・評判を参考として判断するべきです。
- アンチウイルスベンダー各社等も、Windows等と同様にAndroid・iOS向けにもセキュリティアプリをリリースしていますが、そのような「本物のアプリ」であることを周辺の情報等で十分確認した上でインストールを検討することが重要です。

NTT docomo

ドコモからのお知らせ

【注意喚起】セキュリティソフトを装ったフィッシングSMSやアプリにご注意ください

2022年8月26日

平素はNTTドコモの商品・サービスをご利用いただき、誠にありがとうございます。

悪意のある第三者が「お客様の端末から異常ログイン」「必ずセキュリティソフトをアップデート」「お客様の端末からウィルスが検出」などと記したSMSを発信し、そこに記載されたURLのリンク先からセキュリティアプリを装った不審なアプリ（「スマホ安心セキュリティ」など）のインストールを促し、さらにネットワーク暗証番号の入力も促す事案が確認されています。また、不審なアプリをインストールすることによりお客さまに意図せぬ決済が発生する事案も確認されています。不審なSMS、アプリにはくれぐれもご注意ください。

<発見された不審なセキュリティアプリの画面の例>

●危険度はDirty Pipe並み？8年間見つかっていなかったLinuxカーネルの脆弱性

https://news.mynavi.jp/techplus/article/20220823-2432242/
https://thehackernews.com/2022/08/as-nasty-as-dirty-pipe-8-year-old-linux.html
https://news.mynavi.jp/techplus/article/20220819-2428756/

このニュースをザックリ言うと・・・

- 8月22日(現地時間)、「The Hacker News」より、Linuxカーネルにおいて8年間未発見だった脆弱性「CVE-2022-2588」が発見されたと報じられました。

- 脆弱性はノースウェスタン大学の研究者グループが発見したもので、悪用により、サーバー上の攻撃者がローカルから管理者権限を奪取し、サーバー全体の乗っ取りを行うことが可能とされています。

- 同グループは8月17日に当該脆弱性を悪用する「DirtyCred」と名付けられた攻撃手法をセキュリティカンファレンス「Black Hat」で発表しており、3月に発表された「Dirty Pipe(CVE-2022-0847)」と同様に厄介なものと評価され、CVSSによる危険度のスコアも同じく7.8となっています。

AUS便りからの所感

- DirtyCredについては、前述のCVE-2022-2588の他、2021年に修正済みの別の脆弱性(CVE-2021-4154)を悪用するものも発表されています。

- Dirty Pipeで悪用される脆弱性と同様、Webサービス等を介して直接悪用することは基本的に不可能ですが、他の脆弱性を悪用してサーバー上へ侵入した攻撃者による悪用の他、サーバー上にログイン可能なユーザーに悪意を持つものがいるケースに注意が必要です。

- Linuxディストリビューションでは現在DebianとUbuntuについてカーネルのセキュリティアップデートがリリースされており、他のディストリビューションにおいても今後同様のアップデートがあり次第適用すること、またLinuxカーネルはこれ以外にも頻繁に脆弱性が報告されているため、各種ソフトウェアを含めディストリビューションから提供されるパッケージを最新バージョンに保つ管理体制を整えることが肝要です。


TECH+ Powered by マイナビニュース

Linuxカーネルに厄介な8年ものの脆弱性を発見

2022/08/23 14:51　著者：後藤大地

The Hacker Newsは8月22日(米国時間)、「"As Nasty as Dirty Pipe" — 8 Year Old Linux Kernel Vulnerability Uncovered」において、Linuxカーネルに8年前から存在する脆弱性が発見されたと伝えた。発見したセキュリティ研究グループはこのセキュリティ上の脆弱性を「Dirty Pipe」と同じくらい厄介と述べている(参考「Linuxに特権昇格の脆弱性「Dirty Pipe」、アップデートを | TECH+（テックプラス）」)。

ノースウェスタン大学の研究者グループによってLinuxカーネルに「DirtyCred」と名付けられた脆弱性があることが明らかとなった。これまで知られていなかった欠陥(CVE-2022-2588- Red Hat Customer Portal)を悪用し、特権を最大レベルまでエスカレートさせるとされている。

●個人情報3万人以上保存された電子カルテ用PC、修理対応時に紛失か

https://www.itmedia.co.jp/news/articles/2208/24/news193.html
https://www.spch.izumo.shimane.jp/

このニュースをザックリ言うと・・・

- 8月22日(日本時間)、島根県より、同県立中央病院の患者の個人情報が保存されていた電子カルテ用端末PCを紛失したと発表されました。

- 端末に保存されていたのは、2020年8月27日～2021年1月26日に同病院で受診または入院した患者24,563人分の情報および端末を利用する職員情報6,180人分で、現時点でこれらの情報が外部に漏洩した事実は確認されていないとのことです。

- 同病院では、端末が故障したことを受けて2021年3月9日に修理業者にこれを引き渡しており、その後で紛失した蓋然性が高いとしている一方、業者側は引き渡しに関する書類のやり取りがないため、受け取ったと断言できない等と主張しているとのことです。

AUS便りからの所感

- 同病院では「端末にデータを保存したまま修理に出していたこと」や「機器故障時の修理手順を定めておらず、修理発注時に機器の受領書を徴していなかったこと」等の問題が、端末の紛失によって個人情報の流出に至りかねない可能性が発生した原因であることを認めており、再発防止策として「端末を業者に引き渡す際の記憶装置の取り外しを徹底」「業者からの受領書の徴収」その他を挙げています。

- 端末上に受信したデータが保存される仕様となった運用上の理由も発表において説明されていますが、これに対し、一切データを保存しない仕様でなくとも、例えば端末上ではデータが暗号化される等を検討していれば、端末が紛失した場合のリスクは抑制されていた可能性もあります。

- 今回の件とは関係なく、例えばPC等を受け取った修理業者や廃棄業者の中にHDD等から情報を吸い出そうとする者がいる可能性を考慮するならば、OSが提供するようなデータ暗号化機能を活用してデータを保護することは有用です(ただしその機能については十分に把握し、回復キー等は必ずどこかに保存しておくことを推奨致します)。


ITmedia NEWS

島根の県立病院、約2万5000人分の個人情報入り端末紛失　1年半前から行方不明

2022年08月24日 19時35分 公開　[ITmedia]

島根県は8月22日、島根県立中央病院の患者の個人情報が入った電子カルテ用端末の所在が、1年5カ月以上前から分からない状態だと発表した。患者の個人情報24563人分に加え、職員の情報6180人分を保存していたという。県は端末の捜索を続けるとともに、再発防止策を講じるとしている。

個人情報が保存されている電子カルテ用端末の紛失について

島根県立中央病院において、個人情報が保存されている電子カルテ用端末を紛失する事案が発生しました。

適切に管理しなければならない個人情報が保存されている端末を紛失することは、あってはならないことであり、多大なご迷惑とご心配をおかけしますことを心よりお詫び申し上げます。

今後、端末の捜索を継続するとともに、再発防止の徹底に努めて参ります。

1．概　要

中央病院の患者情報 24,563 人分と端末を利用する職員情報 6,180 人分が保存されている電子カルテ用端末 1 台が故障し、その修理の対応を機に、令和３年３月９日以降、所在が不明となっております。

中央病院としては、調査を進めた結果、①令和３年３月１日に業者へ修理見積の依頼をしていること、②令和３年３月９日に業者から修理品の回収をする旨の連絡があったこと、③同日の病院出退管理簿に業者の訪問の記録が残っていること、④