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。

## ●WebP画像の処理における脆弱性が報告…Chrome・Edge他ブラウザー相次いで対応

https://www.itmedia.co.jp/news/articles/2309/14/news076.html
https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html
https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#september-12-2023
https://www.mozilla.org/en-US/security/advisories/mfsa2023-40/
https://stackdiary.com/critical-vulnerability-in-webp-codec-cve-2023-4863/

### このニュースをザックリ言うと・・・

- 9月11日(現地時間)、米Google社より、同社開発のChromeブラウザーの最新バージョン116.0.5845.187/.188(Windows)および116.0.5845.187(Mac・Linux)において、WebP画像処理における脆弱性「CVE-2023-4863」への対策を行ったと発表されました。

- 脆弱性の悪用により、不正なWebP画像を用いてのPCの乗っ取り等の恐れがあるとされ、既に攻撃コードも確認されているとしています。

- 同12日には、Edge(116.0.1938.81)・Firefox(117.0.1)等のWebブラウザーでも相次いでセキュリティアップデートがリリースされています。

- IT系メディアStackDiaryによれば、脆弱性は2014年から存在しており、ブラウザー以外でもWebPライブラリを使用して画像を取り扱うGIMP等のツールや、Webブラウザーと同様のレンダリングエンジンを利用するデスクトップアプリ等、影響範囲は多岐にわたるとしています。

### AUS便りからの所感等

- WebPはGoogleが2010年に仕様および各種ツールを公開した画像フォーマットで、近年はTwitter(現:X)等での画像表示時にJPEGの代わりに利用される場面があります。

- StackDiaryが例に挙げるアプリケーションにはThunderbird(115.2.2で修正)のようなメーラー、Telegram・Signalのようなメッセージアプリケーションがあり、攻撃者が不正なWebPを添付したメール・メッセージ等を無差別に送信する攻撃を想定しているとみられます。

- 脆弱性は9月6日にApple社のセキュリティ研究チーム等からGoogleに報告されたもので、Apple製各種製品でも同様の脆弱性が修正されたとみられています(正式な発表は確認されていません)。

- 最低でも使用しているブラウザーが最新バージョンであることを確認(Chrome・Edgeも9/20現在117系が最新です)し、アンチウイルスとそのパターンファイルも最新に保つこと、他のアプリについても脆弱性が影響しないか確認するとともにやはり最新バージョンに保つよう心掛けることが肝要です。

ITmedia NEWS

### WebPコーデックの重大な脆弱性対処でChromeなど主要Webブラウザが緊急更新

2023年09月14日 06時38分 公開　[ITmedia]

米GoogleのChromeや米MicrosoftのEdgeなど、主要Webブラウザが9月11日から重大なゼロデイ脆弱性に対処するアップデートをリリースしている。この脆弱性「CVE-2023-4863」は、GoogleのWeb向け画像フォーマット「WebP」のヒープバッファオーバーフローに関するもので、既に悪用されているという。

この脆弱性は、米Apple Security Engineering and Architecture（SEAR）と加トロント大学のCitizen Labが6日に報告した。

本稿執筆現在、Chrome、Mozilla Firefox、Brave、Microsoft Edgeがこの脆弱性に対処するアップデートをリリースしている。

Googleは公式ブログで、「CVE-2023-4863のエクスプロイトが存在することを認識している」とした。

## ●三井住友銀行、詐欺メールに見立てた注意喚起メール送信が話題に

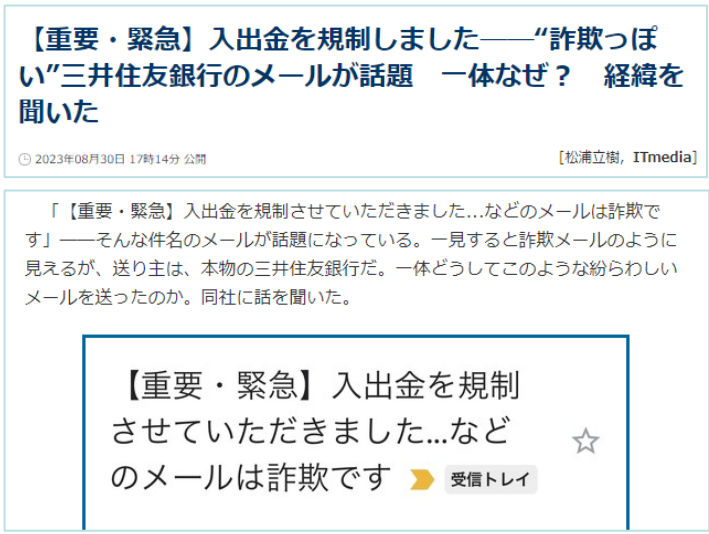
https://www.itmedia.co.jp/news/articles/2308/30/news163.html
https://www.smbc.co.jp/security/attention/index36.html

### このニュースをザックリ言うと･･･

- 8月30日(日本時間)、三井住友銀行より詐欺メールに似た文面のメールが送信され、SNS上で話題となっています。
- 送信されたメールの本文は「お客さまの口座の入出金を規制させていただきましたので、お知らせします。本人確認後、制限を解除することができます」で始まったうえで、このような文面で偽のログイン画面等へのボタン・リンクをクリックさせようとする詐欺メール・SMSへの注意喚起を促す内容となっています。
- メールでは、同行から「入出金規制」「不正利用」等不安を煽る内容や、文中に記載されたボタン・リンクからログイン画面に誘導することはないとしています。

### AUS便りからの所感

- SNSでの反応は賛否両論でしたが、送信されたメールには公式サイトあるいはフィッシングサイトに見立てた特設サイト等へのリンクやURLの記載はなく、注意喚起に際し同行が伝えたいことが本文中に一通りまとまっていたことを評価する声もありました。
- 企業・組織によっては、自組織内で、あるいは外部サービスの提供のもとフィッシング等の訓練を行っている所も少なからずあると思われますが、訓練の段階で罠を踏んでしまったユーザーも萎縮させることなく、全体でフィッシングを確実に回避できるようなリテラシーを養える内容とすることが望まれます。




## ●ダウンロードツール「Free Download Manager」公式サイトに不正アクセス、偽の配布サイトへリダイレクト

https://news.mynavi.jp/techplus/article/20230917-2772562/
https://securelist.com/backdoored-free-download-manager-linux-malware/110465/
https://www.freedownloadmanager.org/blog/?p=664

### このニュースをザックリ言うと･･･

- 9月12日(現地時間)、セキュリティベンダーのカスペルスキー社より、ダウンロードツール「Free Download Manager(以下・FDM)」の公式サイトが不正アクセスを受け、同ソフトのLinux版ダウンロード時に外部の偽サイトへ誘導される状態にあったことが発表されました。
- 同社が調査していた「fdkpkg.***」という不審なドメイン名のもとで「deb.fdmpkg.***」という偽のFDM配布サイトが稼働しており、配布されていたマルウェア入りLinux版パッケージのインストールにより、PC上にバックドアが設置されることが確認されたとのことです。
- また、少なくとも2020年から2022年にかけて、FDMの公式サイトからLinux版をダウンロードしようとした際に「deb.fdmpkg.***」上のマルウェア入りパッケージをダウンロードするよう仕掛けられていたことが、ネット上の掲示板等で確認されたとしています。
- 同13日にはFDMの公式サイトにおいてこの事象を認める声明が発表されており、サイト訪問者の0.1%未満が影響を受けた可能性があるとし、また2022年に事象に気付かないままサイトの更新を行ったことで解消されたとしています。

### AUS便りからの所感

- 2020年10月にYouTubeに投稿されたLinux版FDMのインストール動画において、偽サイト上のマルウェア入りパッケージをダウンロードするよう誘導される様子が確認されている一方、同時期の動画でこのような誘導が発生していないケースもあり、一定の確率ないし特定の条件下で誘導が発生した可能性があるとされています。
- 不正アクセスによるとみられるWebサイトの改ざん事案は先日も国内で多発しており(AUS便り 2023/09/13号参照)、この時は偽のメッセージを表示するものでしたが、今回のようにマルウェアをダウンロードするよう誘導される等、さまざまな被害をもたらす恐れもあります(いわゆる「サプライチェーン攻撃」の一つとも言えます)。
- Webサーバー自体はもちろん、サイト管理人のPCにおいても不正アクセスによる侵入を防ぐようOS・アプリ等を最新に保つことは重要であり、また改ざんを検知する内外のソリューションの導入も検討に値するでしょう。