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。

● 「BeReal」で職場内を撮影した動画流出、銀行が謝罪

https://www.itmedia.co.jp/news/articles/2604/30/news096.html
https://www.ncbank.co.jp/assets/a5d6dd906a3c43e5bbf96d8adc3d2a13/8d0eab990c95489db41bcd1b4185802e/osirase260430-01.pdf
https://www.itmedia.co.jp/news/articles/2604/30/news111.html
https://www.itmedia.co.jp/news/articles/2604/30/news135.html

このニュースをザックリ言うと･･･

- 4月30日(日本時間)、西日本シティ銀行より、同行職員が支店の執務室内を撮影した動画がX(旧Twitter)上で拡散していたと発表されました。

- 動画は元々2024年にSNSアプリ「BeReal」で撮影・投稿されたものとみられ、第三者が保存していたものが4月29日以降にX上で拡散したとみられています。

- 動画には執務室内のホワイトボード上に記載された顧客数名の氏名が映っていたことから、該当者に個別に謝罪・説明を行うとしています。

- この事案が報じられたのと前後して、BeRealによる製造業・食品チェーン店等の内部あるいは学校教員の自宅勤務中の撮影動画等に、個人情報や取引先情報が映り込んでいたとする事案が相次いでいます。

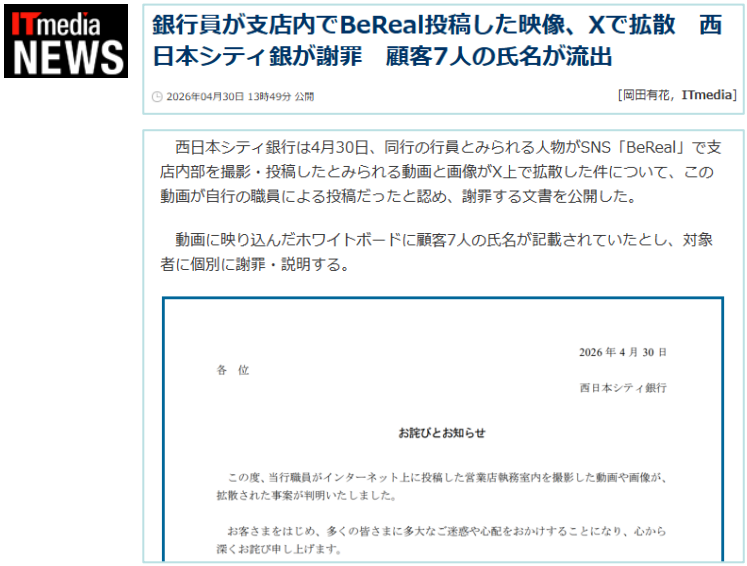
AUS便りからの所感等

- BeRealには、毎日不特定の時間に通知を受け、2分間の間に動画を撮影して投稿するルール(投稿しなかった場合は他のユーザーの動画が閲覧できなくなる)があり、意図しないプライバシーの侵害・個人情報等が写される恐れがあることが日本でも懸念されていました。

- また投稿した動画は24時間で削除される仕様とされていた一方、今回のように動画を保存して数年後に(恐らくは悪意を以て)拡散させる者がいることや、利用規約に「投稿された動画・画像をBeReal運営が無償で再利用する権利を有する」とする条項が書かれていたことも話題となっています。

- 機密情報の管理に厳しくあるべき場に私用のスマートフォンの持ち込みが行われたことについても批判に値しますが、今回の事案がセンセーショナルに報じられたことで、今後他業種でも私用機器の持ち込みの禁止のみならず、さらには職場に持ち込まれないスマートフォンも含めこのようなアプリのインストールを制限するような、考え方によっては「過剰な規制」も行われる可能性が憂慮されます。

- そもそもBeReal自体、インストールしたスマートフォンにマルウェアを感染させるような露骨なものではないとしても、ペナルティ回避のため時には危険となり得る行為を短時間で実行するよう脅す仕様はあまりにも危険と言え、各種SNS等との付き合い方について、ユーザー側から真剣に考え直す機会となることを切に望みます。



ITmedia NEWS

銀行員が支店内でBeReal投稿した映像、Xで拡散　西日本シティ銀が謝罪　顧客7人の氏名が流出

2026年04月30日 13時49分 公開　[岡田有花，ITmedia]

西日本シティ銀行は4月30日、同行の行員とみられる人物がSNS「BeReal」で支店内部を撮影・投稿したとみられる動画と画像がX上で拡散した件について、この動画が自行の職員による投稿だったと認め、謝罪する文書を公開した。

動画に映り込んだホワイトボードに顧客7人の氏名が記載されていたとし、対象者に個別に謝罪・説明する。

2026 年 4 月 30 日

各　位

西日本シティ銀行

お詫びとお知らせ

この度、当行職員がインターネット上に投稿した営業店執務室内を撮影した動画や画像が、拡散された事案が判明いたしました。

お客さまをはじめ、多くの皆さまに多大なご迷惑や心配をおかけすることになり、心から深くお詫び申し上げます。

● Linuxカーネルに脆弱点「Copy Fail」、ローカルからサーバー乗っ取りの可能性

https://japan.zdnet.com/article/35247165/
https://www.ipa.go.jp/security/security-alert/2026/alert20260501.html
https://www.walbrix.co.jp/article/copy-fail-cve-2026-31431.html

このニュースをザックリ言うと・・・

- 4月29日(現地時間)、Linuxカーネルに危険度の高い脆弱点「Copy Fail」(CVE-2026-31431)が存在すると発表されました。
- 2017年にリリースされたバージョン4.14以降のカーネルが影響を受けるとされ、悪用により、ローカル攻撃者がroot(管理者ユーザー)権限を奪取し、サーバーを乗っ取ることが可能とされており、5月1日にはIPAからも注意喚起が出されています。
- 5月8日現在、各種Linuxディストリビューションにお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、アップデートもしくは回避策の適用が推奨されています。

AUS便りからの所感

- 脆弱点の悪用は基本的にローカルからのみ実行可能であり、通常はWeb・メールサーバーに対し直接脆弱点を突くことはできず、攻撃者がSSH等でサーバーにログイン可能であることが攻撃の条件とされます。
- 一方でCopy Failを発見した研究者により、脆弱点を悪用する攻撃コードが配布されていますが、極めて簡単なスクリプトでできている模様で、サーバーにログイン可能な攻撃者が攻撃ツールを持ち込むことは難しくはないと考えられます。
- Copy Failの原因は特定のモジュールに存在しており、Copy Failの発見者のWebサイトではすぐにアップデートが適用できない場合の回避策(当該モジュールのロードを遮断する、およびロード済みの場合はアンロードする)が提示されていますが、RHELおよび派生ディストリビューション(Rocky Linux, Almalinux等)では別の回避策(ブート時のパラメータを設定)をとる必要がある等、十分な情報収集の上で対策を実施すること、またこのような脆弱点に限らず普段からの攻撃の可能性を抑止するため、SSHはじめサーバー管理用のサービスポートについては可能な限りアクセス元IPアドレスの制限等を行うことを強く推奨致します。
- なお5月7日には、やはりローカルからの攻撃でroot権限の奪取が可能とされる別の脆弱点「Dirty Frag」が報告され、近日中に再びカーネルのセキュリティアップデートが見込まれており、カーネルから各種ソフトウェアまでアップデートを適切に実施できる体制を整えることが肝要です。

ZDNET

「Linux」に極めて重大な脆弱性--「Copy Fail」発覚

Jack Wallen (Special to ZDNET.com) 翻訳校正： 2026-05-06 03:24

「Copy Fail」として知られる「CVE-2026-31431」は、2017年から潜伏していた「Linux」カーネルの深刻な脆弱（ぜいじゃく）性であり、現在セキュリティ上の大きな注目を集めている。通常、Linuxの脆弱性は過大評価される傾向にあるが、今回のケースは例外といえる。Copy Failは極めて重大な問題であり、速やかな対策を講じる必要がある。

この脆弱性は、特定のデータ形式のセキュリティ処理を担うLinuxシステム上の欠陥に起因する。システムへの基本的なアクセス権限を持つ攻撃者が、コンピューターのRAM内に存在する極めて重要なデータを改ざんすることを可能にする。この改ざんが行われると、システムは攻撃者をrootユーザーであると誤認し、攻撃者にシステム全体の完全なコントロール権限を与えてしまう。

これまでLinuxを襲った他の脆弱性とCopy Failが異なる点は、攻撃の実行に際して特定のタイミングや複雑な手順を必要としないことにある。攻撃の難易度が極めて低い一方で、その影響は壊滅的なものになりかねない。

● Apache HTTP Server 2.4.67リリース、11件の脆弱点修正

https://forest.watch.impress.co.jp/docs/news/2106854.html
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.67
https://jvn.jp/vu/JVNVU99705957/

このニュースをザックリ言うと・・・

- 5月4日(現地時間)、Apache Software Foundationより、Apache HTTP Server(以下・Apache)の最新バージョン2.4.67がリリースされています。
- 11件の脆弱点を修正したセキュリティアップデートで、HTTP/2プロトコルの処理上で任意のコード実行が可能となる脆弱点(CVE-2026-23918)が特に危険度が高いとされ、他にも一部のモジュールに対し、サービス拒否(DoS)状態に陥る、特定の認証機能を回避される、メモリの一部が漏洩する等の脆弱点が指摘されています。
- 同8日にはJPCERT/CCからも注意喚起が出されています。

AUS便りからの所感

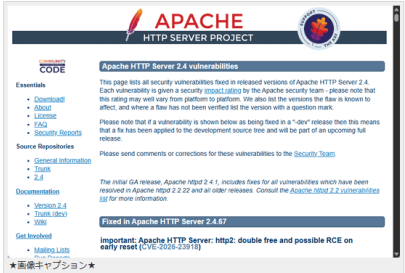
- Apacheでは不定期にセキュリティアップデートがリリースされ、今回は2.4.66以来5ヶ月ぶりのバージョンとなります。
- 前述のCVE-2026-23918は2.4.66にのみ影響する脆弱点であり、RHELおよび派生ディストリビューション(Rocky Linux, Almalinux等)等、当該バージョンをベースとしていないものについては、影響を受けないとされています(2.4.66をソースコードからコンパイルした場合は、アップデートの実施もしくは回避策としてHTTP/2の無効化が必要です)。
- 5月8日現在、DebianおよびUbuntuについてはパッケージが更新されており、RHELおよび派生ディストリビューションについてもアップデートがリリースされ次第、適用が推奨されます。
- Apacheからの移行先として既に人気の高いnginx等でも時々セキュリティアップデートがリリースされる(例えば3月には6件の脆弱点が修正されています)ため、どんなソフトウェアを使用していてもセキュリティアップデート等は付いて回るものと留意し、サーバーを安全に保つための運用体制を整えましょう。

Impress Watch

「Apache HTTP Server」にセキュリティ修正 ～リモートコード実行の恐れがある脆弱性

最大深刻度Importantの脆弱性2件を含む計11件を修正したv2.4.67がリリース

長谷川 正太郎　2026年5月8日 06:45



★画像キャプション★

The Apache Software Foundationは7月1日、「Apache HTTP Server 2.4.67」を公開した。以下に挙げる11件の脆弱性を修正したセキュリティアップデートとなっている（カッコ内は同団体の基準による深刻度）。

▪ CVE-2026-23918：http2: double free and possible RCE on early reset（i