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。

●関西万博チケット、不正アクセスによる第三者への譲渡事例が報じられる

https://www.sankei.com/article/20250915-A3PW7R422JPLBPOIE4IN6I7FFA/
https://www.fnn.jp/articles/-/933876
https://www.mbs.jp/news/feature/specialist/article/2025/09/108275.shtml

このニュースをザックリ言うと･･･

- 9月15日以降(日本時間)、複数メディアにおいて、大阪・関西万博の電子チケットが、不正アクセスにより第三者に譲渡される事例が確認されたと報じられています。
- 報道によれば、万博のチケットサイトへ不正にログインされ、家族・知人にチケットを譲渡する機能を悪用されたとみられます。
- 万博のチケットをめぐっては、チケットサイトへ短時間に多数のログイン試行を行ったところ、ID(万博ID)を停止されたというトラブルも多く報告されています。

AUS便りからの所感等

- チケットサイトにおいては、万博IDとパスワードによるログインの他、本人確認方法として「登録メールアドレスへ送信されるワンタイムパスワード」「アプリが生成するワンタイムパスワード(TOTP)」および「生体認証」が利用可能です。
- 不正ログインにおいては、十分に強力ではないパスワードを設定していた、他のサイトで使用していたパスワードを使い回していた(これによりパスワードリスト攻撃を受けた)可能性、またワンタイムパスワードによる本人確認の際、フィッシングサイトにID・パスワードおよびワンタイムパスワードを入力してしまい、奪取された可能性、等が考えられます。
- 不正ログインを最も確実に防ぐためには、基本的に登録したスマートフォンからのみログイン可能となるパスキーによる認証を選ぶことが望ましく、それ以外を用いる場合は、パスワードマネージャー等が生成した十分に複雑ないし長いパスワードを用いる、かつフィッシングの可能性に対し十分に注意を払うことが肝要です。

THE SANKEI NEWS

不正アクセスで万博のチケットを第三者に譲渡　協会は「パスワードの管理を」と注意喚起

2025/9/15 19:31

ポスト　反応　記事を保存

社会 | 事件・疑惑　2025年大阪・関西万博

万博会場の大屋根リング＝大阪市此花区の夢洲

日本国際博覧会協会（万博協会）は15日、大阪・関西万博の電子チケットの購入者が、無断でチケットを他人に譲渡されたケースを確認したと明らかにした。譲渡に必要な個人IDやパスワードが流出し、チケットサイトへアクセスされた可能性があるという。

万博協会の高科淳副事務総長は同日の記者会見で「パスワードの管理をしっかりおこなってほしい」と呼び掛けた。

万博のチケットサイトには、家族や知人などにチケットを譲渡できる機能がある。高科氏によると、この機能を何者かが不正に利用し、無断でチケットを他人に譲渡されるトラブルが発生しているのを確認したという。

● 7-Zipにシンボリックリンク処理に関する問題…最新バージョン25.01で対策済み

https://forest.watch.impress.co.jp/docs/news/2049280.html
https://lunbun.dev/blog/cve-2025-55188/

このニュースをザックリ言うと･･･

- 8月28日(現地時間)、アーカイブ作成・解凍ソフト「7-Zip」に脆弱性(CVE-2025-55188)が存在していたことが、発見者のlunbun氏より発表されました。

- 脆弱性は書庫ファイルに含まれるシンボリックリンクの展開処理に存在し、細工されたファイルの展開時に外部のディレクトリ上にあるファイルの上書き等を行われる可能性があったとしています。

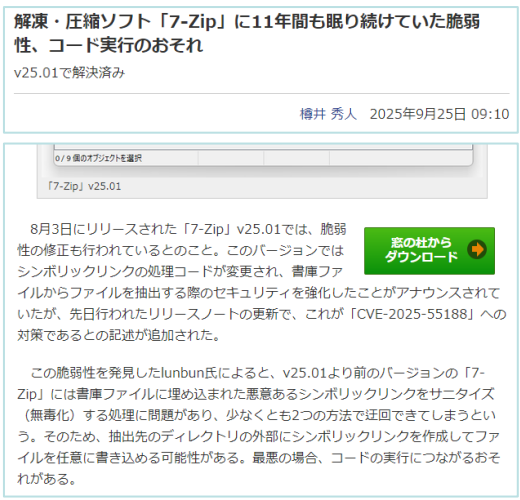
- 脆弱性はlunbun氏から7-Zipの開発者へ報告されており、8月3日にリリースされた最新バージョン25.01で修正済みとのことで、バージョン25.00以前を利用しているユーザーに対しアップデートが呼び掛けられています。

AUS便りからの所感

- シンボリックリンクはLinuxでは一般的な機能である一方、過去にも様々なソフトウェアで、外部ディレクトリを指すリンクの作成により、任意のファイルを上書きするよう攻撃される脆弱性が報告されています。

- Windowsでは通常シンボリックリンク作成のために管理者権限が必要であること等から、CVE-2025-55188の危険度は比較的低く設定されている模様ですが、管理者として書庫ファイルを展開する場面は少なからず存在し、これを狙って不正な書庫ファイルによる攻撃を行うシナリオが考えられます。

- 7-Zipのような自動更新ないしアップデートリリース時の通知を行う機能がないソフトウェアについては、アップデートのリリース情報を随時収集しつつ、また最新バージョンの入手の際にもサーチエンジンで上位に表示されたサイトに安易にアクセスすることなく(偽のソフトウェアやマルウェアをダウンロードさせる悪意のあるサイトが広告で表示される場合があるため)、ソフトウェア自身のバージョン情報等で表示される公式サイトへアクセスすることに留意すべきでしょう。



●8月度フィッシング報告件数は193,333件…6か月連続で19万件超

https://www.antiphishing.jp/report/monthly/202508.html

このニュースをザックリ言うと･･･

- 9月22日(日本時間)、フィッシング対策協議会より、8月に寄せられたフィッシング報告状況が発表されました。

- 8月度の報告件数は193,333件で、7月度(https://www.antiphishing.jp/report/monthly/202507.html)の226,433件から33,100件減少しています。

- 悪用されたブランド件数は99件で7月度(96件)から2件増加、割合が多かったものとしてSBI証券(約12.3%)、Amazon(約12.0%)が挙げられ、次いで1万件以上報告されたApple、AMEX、ANAと合わせて約44.8%、さらに1,000件以上報告された34ブランドまで含めると約94.6%を占めたとのことです。

- フィッシングサイトのURL件数は76,283件で7月度(85,272件)から8,989件減少、使用されるTLD(トップレベルドメイン名)の割合は10,000件以上の報告があった .com(約47.5%)、 .cn(約21.9%)、 .top(約10.5%)、で約79.9%を占めています。

AUS便りからの所感

- 3月度に過去最多の249,936件となって以降、報告件数は19万件超の状態が続いています。

- 1,000件以上報告されたブランド数については6月の27ブランドから7月に35ブランドと急増、8月も多数のブランドが狙われる状況が続いているとしています。

- また日本データ通信協会の迷惑メール相談センターには日々20件以上のフィッシングメールが掲載されており(https://www.dekyo.or.jp/soudan/contents/news/alert.html)、利用しているサービスについて不審なメールを受信した際はこういった情報等と文言が一致するか確認するとともに、本物のサービスのサイトへは事前に登録したブラウザーのブックマークやスマホアプリからアクセスする等、慎重に行動することを日々心掛けましょう。