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。

●ポケモンセンターオンラインでリスト型攻撃、全アカウントでパスワードリセット措置

https://ascii.jp/elem/000/004/296/4296938/
https://www.pokemoncenter-online.com/news/?id=20250703_1

このニュースをザックリ言うと･･･

- 7月3日(日本時間)、株式会社ポケモンより、同社が運営する「ポケモンセンターオンライン」への不正ログインを確認したと発表されました。
- 不正ログインはいわゆる「リスト型攻撃」による可能性があるとされ、被害を受けたアカウントのメールアドレス・氏名・住所・電話番号・生年月日等が閲覧あるいは書き換えられた可能性等があるとしています(クレジットカード情報は対象外とのことです)。
- 同社では不正ログインの被害を受けたもの含め全てのアカウントについてパスワードリセットを行っており、一部会員情報の書き換えが発生したアカウントは停止処置をとったとのことです。
- また、8月頃を目途にログイン時の二段階認証を導入するとしています。

AUS便りからの所感等

- リスト型攻撃の事案は数えきれないほど発表され、「推測されやすいパスワード」「複数のサービス間でパスワードの使い回し」等を避けるようユーザー側での自衛が度々呼び掛けられています。
- 今日、パスワード管理ツールの利用とこれを用いた複雑なパスワードの設定ももはや特殊なケースではなくなっている一方、リスト型攻撃を中心とした不正ログインへの対策をユーザー側のみに帰すことなく、サービス側でも二段階認証等の導入をとるよう求められるフェーズに入っているものと感じられます。
- 今回、特に子どものユーザーの割合が多いと思われるポケモン関連で発生した事案であり、安全なパスワードがどれだけ設定されるか未知数な上、二段階認証の導入後もフィッシング等によるアカウント情報や二段階認証のための情報(メールで送られてくるコード等)を奪取する攻撃に注意するよう十分に啓発できるかが注目されるところです。

ASCII.jp

ポケモンセンターオンライン、情報漏えいか　全会員のパスワードをリセット

2025年07月03日 15時20分更新　文● Zenon／ASCII

数日振りに再開したポケセンオンライン

ポケモンは7月3日、長期間にわたって緊急メンテナンスを実施し、サービスを停止していたグッズ販売サイト「ポケモンセンターオンライン」のサービス再開を発表した。

緊急メンテナンスの理由は不正ログイン。不審なログインが多数発生していることを確認したため、被害拡大を防ぐ意味で緊急メンテを行っていたとのこと。

今回のサービス再開にともない、会員のアカウントの安全を考慮して「全アカウントのパスワードをリセット」したという。なお、第三者から書き換えがあったと疑われるアカウントは停止された。

●高校受験模試の運営サイトに不正アクセス、個人情報322,000件流出か

https://www.itmedia.co.jp/news/articles/2507/04/news067.html
https://www.zenkenmoshi.jp/

このニュースをザックリ言うと･･･

－6月30日(日本時間)、「愛知全県模試」を運営する学悠出版株式会社より、同社Webサイトが不正アクセスを受け、個人情報の一部が流出した可能性があると発表されました。

－被害を受けたのは、塾関係者のべ約8,000件の塾名・住所・電話番号・メールアドレスおよび担当者氏名、模試受験生約314,000件の氏名(保護者名含む)・塾情報・住所・電話番号およびメールアドレス等、併せて約322,000件とされています。

－4月下旬に不正アクセスについて認知し、SQLインジェクションの脆弱性を突かれたのが原因としています。

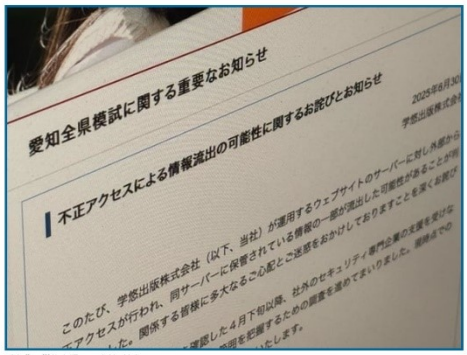
－なお流出した情報のうち受験生に関するものの多くは暗号化されているとのことです(同社所有のデータベースと照合しない限り個人の識別ができないものもあるとしています)。

ITmedia NEWS

「愛知全県模試」の学悠出版に不正アクセス　受験生ら32万件の個人情報漏えいか

2025年07月04日 10時51分 公開　[ITmedia]

愛知県内の高校を受験する中学生を対象とした模擬試験「愛知全県模試」を運営する学悠出版は、自社Webサイトが外部からの不正アクセスを受け、塾関係者や受験生ら約32万2000件の個人情報が流出したおそれがあると発表した。現時点でこれらの情報が不正に利用された報告は確認されていない。



(出典：学悠出版のWebサイト)

内訳は塾関係者が約8000件、模試の受験生が約31万4000件。流出の可能性がある個人情報は、主に塾関係者の氏名やメールアドレス、電話番号、住所など。受験生の氏名や住所なども流出した可能性はあるが、多くは暗号化していたり、学悠出版が保有するデータベースと照合しない限り個人を特定できないものだとしている。

AUS便りからの所感

－SQLインジェクションは単にデータベースからの情報奪取のみならず、Webサイトを改ざんし、フォームに入力された個人情報・決済情報を抜き取るよう仕掛ける等にも悪用される可能性があり、根本的な対策として、Webアプリケーション開発の時点でSQLインジェクション等の脆弱性が入り込まないようにすることが肝要です。

－多重防御の意味では、今回も行われていたようなデータベース上でのデータ暗号化の他、脆弱性を悪用するような不正なWebリクエストあるいは内部からの非正規な情報送信を検知、遮断するようなWAF・IDS・IPSの採用も、十分検討に値します。

●Microsoft等月例のセキュリティアップデート…Win10無償アップデートはあと4回

https://forest.watch.impress.co.jp/docs/news/2029555.html
https://msrc.microsoft.com/blog/2025/07/202507-security-update/
https://forest.watch.impress.co.jp/docs/news/2029681.html
https://forest.watch.impress.co.jp/docs/news/2029791.html

このニュースをザックリ言うと･･･

－7月9日(日本時間)、マイクロソフト(以下・MS)より、Windows・Office等同社製品に対する月例のセキュリティアップデートがリリースされています。

－Windowsの最新バージョンはWindows 10 22H2 KB5062554(ビルド 19045.6093)、11 23H2 KB5062552(ビルド 22631.5624)および11 24H2 KB5062553(ビルド 26100.4652)等となります。

－SQL Serverの情報漏洩の脆弱性(CVE-2025-49719)について攻撃手法が公知となっている他、Office・SharePointおよびAMD製CPUに起因するもの等計12件が特に危険度が高い(4段階中最高の「Critical」)と評価されています。

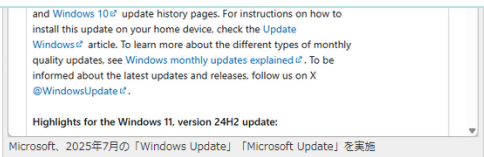
AUS便りからの所感

Impress Watch

Microsoft、2025年7月の「Windows Update」を実施 ～「Office」やAMD CPUの致命的問題にも対処

ゼロデイを含む130件の脆弱性を修正

樽井 秀人　2025年7月9日 08:22



Microsoft、2025年7月の「Windows Update」「Microsoft Update」を実施

米Microsoftは7月9日（現地時間）、すべてのサポート中バージョンのWindowsに対し月例のセキュリティ更新プログラムをリリースした（パッチチューズデー）。現在、「Windows Update」や「Windows Update カタログ」などから入手可能。Windows以外の製品も含め、今月のパッチではCVE番号ベースで130件（サードパーティーのものも含めれば140件）の脆弱性が新たに対処されている。

－Windows 10については、10月の無償サポート期限まで今回を含めあと4回の月例アップデートが予定されている一方、拡張セキュリティ更新プログラム(ESU)も7月に提供開始がアナウンスされ(AUS便り 2025/06/30号)ており、最終的な11への移行について10月までに完了させるか、ESUによる延命を行うか、また後者の場合もその提供・適用条件等を十分に調査した上で早々に計画を立てるべきです。

－同9日にはAdobe社よりIllustrator・Indesign等13製品についてセキュリティアップデートがリリース、Zoom社からもZoom WorkPlaceアプリについて脆弱性が発表(7月1日リリースのバージョン6.5.3で修正済み)されています。

－また16日にはOracle社からJava等について四半期ごとのアップデートリリースが予定されており、システム管理者においてはソフトウェアベンダー各社が定期的に行うアップデートを意識し、OS・ファームウェアないし各種アプリケーションのアップデートと、アンチウイルス・UTM等による多重防御を適切に行うことを常に心掛けましょう。