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。

●GmailのID・パスワード4,800万件等が発見、過去流出したものか

https://forbesjapan.com/articles/detail/90389
https://www.expressvpn.com/blog/149m-infostealer-data-exposed/

このニュースをザックリ言うと・・・

- 1月25日(日本時間)、「Forbes JAPAN」誌のWebサイトにおいて、複数のネットサービスから流出したとみられる149,404,754件のID・パスワード情報がインターネット上のデータベースに公開されていたと報じられています。

- セキュリティ研究者のJeremiah Fowler氏の発表によるもので、主なサービスの内訳としてはGMail約4,800万件、Facebook約1,700万件、Instagram約650万件、Yahoo!約400万件、Netflix約340万件、Outlook約150万件とされています。

- 最近あった新しいセキュリティ侵害によるものではなく、過去に流出した情報を集めたものとされ、また同氏による発見から1か月後にデータベースは非公開にされたとしています。

AUS便りからの所感等

- Forbes JAPANの記事によれば、Googleの広報担当者は、流出した情報を特定した場合、アカウントをロックし、パスワードのリセットを強制するとしています。

- 入力したメールアドレス・パスワードが流出していないか調査するサイト「Have I Been Pwned」に前述のデータが反映されているかについては、記事による識者のコメントでは「まだ早いかもしれない」としながらも、当該サイト等で確認することが強く推奨されています。

- このようなID・パスワード情報のリストを、元のサイトのみならずあらゆるサイトでの不正ログインに使用する、いわゆる「リスト型攻撃」の脅威、またその対策として(適宜パスワード管理ツールも活用しながら)サイト毎に異なった推測されにくい強力なパスワードを設定すること(侵害が確認され次第必ずパスワードを変更すること)は、もう長年の間語られており、今日ではID・パスワードだけによって不正ログインされないための多要素認証(MFA)、パスキーの導入も真剣に検討すべき時期にあるといえます。

Forbes JAPAN

侵害済みアカウントの収集データベースで、Gmailのユーザー名とパスワード4800万件が発見される

Davey Winder | Contributor　著者フォロー　記事を保存　SHARE

高い評価を受けるベテランのセキュリティ研究者ジェレマイア・ファウラーは、約1億4900万件の侵害済み認証情報（推定4800万件のGmailアカウント分を含む）が収録されたデータベースがオンラインで公開されていたことを明らかにした。ファウラーによると、「公開されていたデータベースは、パスワード保護も暗号化も施されていませんでした」という。ユニークなログインとパスワードのデータベースは「生の認証情報データが合計で96GBという巨大な量でした」と付け加えた。現時点で分かっていることと、取るべき行動をまとめる。

> 1億4900万件のログイン認証情報が流出済み――推定4800万件のGmailアカウントを含む

パスワードセキュリティの観点から見ると、新年の出だしは決して良いとはいえない。パスワード管理サービスのLastPass（ラストパス）は攻撃が進行中であることを確認し、数百万人のユーザーに警告を発した。LinkedIn（リンクトイン）ユーザーも、ポリシー違反を口実に使う詐欺師によるアカウントパスワード窃取の標的となり、警戒を強めている。そして今回、保護されていないデータベースで実に1億4900万件もの侵害された認証情報がオンライン上に公開されていたという衝撃的なニュースが飛び込んできた。

新たな侵害ではなく、過去の侵害データやインフォスティーラーのログをまとめたデータベースの可能性

流出したデータベースを発見し、調査結果を報告書として公開したサイバーセキュリティ研究者のジェレマイア・ファウラーによると、このデータベースには合計1億4940万4754件の固有のログイン情報とパスワードが含まれていた。

● IPA「情報セキュリティ10大脅威 2026」、組織側に「AIの利用をめぐるサイバーリスク」初登場

https://www.ipa.go.jp/security/10threats/10threats2026.html

このニュースをザックリ言うと･･･

- 1月29日(日本時間)、IPAより「情報セキュリティ10大脅威 2026」の概要が発表されました。
- 2025年に発生した、社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者等約250名によって、個人と組織それぞれのカテゴリーでの10大脅威を決定しています。
- 今回、組織側の10大脅威において3位に「AIの利用をめぐるサイバーリスク」が初めて入っています。
- 今後、2月下旬以降に詳細の解説が発表される等、追加コンテンツが随時公開される予定となっています。

AUS便りからの所感

- 組織側の10大脅威は、前述の3位と、2年連続選出の6位「地政学的リスクに起因するサイバー攻撃（情報戦を含む）」以外は6回以上選出されたことのある脅威となっており、1位「ランサム攻撃による被害」5位「機密情報を狙った標的型攻撃」6位「内部不正による情報漏えい等」が11年連続ランクインしています。
- 一方の個人側の10大脅威も「インターネットバンキングの不正利用」が4年ぶりに入った以外は、やはり11年連続選出の「インターネット上のサービスへの不正ログイン」「クレジットカード情報の不正利用」「ネット上の誹謗・中傷・デマ」「不正アプリによるスマートフォン利用者への被害」含め9つが7年以上連続で入っており、顔触れは完全に固定されています。
- 12月にJNSAから発表された「2025セキュリティ十大ニュース（https://www.jnsa.org/active/news10/ ）」でも国内で話題になった個々のインシデントが多く取り上げられる等、特に年末年始あるいは半期・四半期においては、大手セキュリティベンダーや関連団体等より、各組織の立ち位置・観点等の違いを少なからず反映した年間のセキュリティ関連ニュースのまとめ、あるいは翌年度等における業界の動向予測等がリリースされますので、自分自身や自組織に関連するもの以外も含め各種脅威について知識を得ること、過去に得た知見についても随時更新していくことを推奨致します。

IPA

情報セキュリティ10大脅威 2026［組織］

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	11年連続11回目
2	サプライチェーンや委託先を狙った攻撃	2019年	8年連続8回目
3	AIの利用をめぐるサイバーリスク	2026年	初選出
4	システムの脆弱性を悪用した攻撃	2016年	6年連続9回目
5	機密情報を狙った標的型攻撃	2016年	11年連続11回目
6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）	2025年	2年連続2回目
7	内部不正による情報漏えい等	2016年	11年連続11回目
8	リモートワーク等の環境や仕組みを狙った攻撃	2021年	6年連続6回目
9	DDoS攻撃（分散型サービス妨害攻撃）	2016年	2年連続7回目
10	ビジネスメール詐欺	2018年	9年連続9回目

情報セキュリティ10大脅威 2026［個人］

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	7年連続10回目
インターネット上のサービスへの不正ログイン	2016年	11年連続11回目
インターネットバンキングの不正利用	2016年	4年ぶり8回目
クレジットカード情報の不正利用	2016年	11年連続11回目
サポート詐欺（偽警告）による金銭被害	2020年	7年連続7回目
スマホ決済の不正利用	2020年	7年連続7回目
ネット上の誹謗・中傷・デマ	2016年	11年連続11回目
フィッシングによる個人情報等の詐取	2019年	8年連続8回目
不正アプリによるスマートフォン利用者への被害	2016年	11年連続11回目
メールやSNS等を使った脅迫・詐欺の手口による金銭要求	2019年	8年連続8回目

●Linuxのtelnetdに脆弱性、サーバー乗っ取りの恐れ

https://thehackernews.com/2026/01/critical-gnu-inetutils-telnetd-flaw.html

このニュースをザックリ言うと･･･

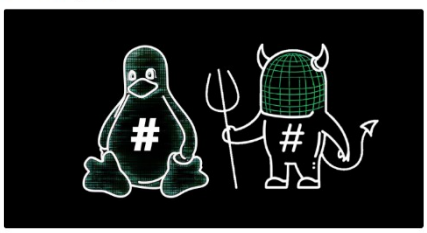
- 1月19日(米国時間)、主にLinuxで使用されるGNU InetUtilsのtelnetdに危険度の高い脆弱点「CVE-2026-24061」が存在することが報告されました。
- 脆弱点の悪用により、Linuxサーバーのroot(管理者)権限の奪取も可能となり、サーバーの乗っ取りの恐れがあるとされています。
- 脆弱点は2015年リリースのInetUtils 1.9.3から最新バージョンの2.7までに存在しますが、telnetdが稼働している場合にのみ有効であり、開発元からは修正パッチが提供されています(修正バージョン2.8は後日リリース予定とみられます)。

AUS便りからの所感

- 1月30日時点で、主なLinuxディストリビューションにおいて、Debianでは修正バージョンがリリースされていますが、Ubuntuではまだリリースされておらず、一方RedHat Enterprise Linux系では影響は受けないとしています(InetUtilsベースのtelnetdを使用していないためとみられます)。
- 今回の脆弱点はGNU InetUtilsに固有とされますが、Linuxサーバーへのリモートログイン用途としては既にSSHが主流であり、telnetポート(TCP21番)をインターネット上で公開するケースはよほど意図的でない限りは皆無と思われる一方、例えばネットワーク機器がLinuxベースで、かつコマンドラインによる管理のためにtelnetサービスが用いられている場合に脆弱性の影響を受ける可能性があり、このようなケースにおいてもベンダーからのパッチリリース等の情報に注視すべきでしょう。
- 大規模なボットネットの構築等を行った「Mirai」のようにIoT機器等のtelnetポートをターゲットとするマルウェアや攻撃者は依然多く存在しており、外部への公開を意図していないポートがアクセス可能でないか確認を行い、サーバー自身や前面のルーター・UTM等によるフィルタリング設定を実施することも肝要です。

The Hacker News

Critical GNU InetUtils telnetd Flaw Lets Attackers Bypass Login and Gain Root Access



A critical security flaw has been disclosed in the GNU InetUtils telnet daemon (telnetd) that went unnoticed for nearly 11 years.

The vulnerability, tracked as CVE-2026-24061, is rated 9.8 out of 10.0 on the CVSS scoring system. It affects all versions of GNU InetUtils from version 1.9.3 up to and including version 2.7.

"Telnetd in GNU Inetutils through 2.7 allows remote authentication bypass via a '-f root' value for the USER environment variable," according to a description of the flaw in the NIST National Vulnerability Database (NVD).

In a post on the oss-security mailing list, GNU contributor Simon Josefsson said the vulnerability can be exploited to gain root access to a target system -