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。

●パスワードの文字を入れ替えた程度の使い回しを推測する攻撃手法、中国の研究者発表

https://www.itmedia.co.jp/news/articles/2309/21/news014.html
https://xtech.nikkei.com/atcl/nxt/column/18/00676/093000150/
https://www.usenix.org/conference/usenixsecurity23/presentation/wang-ding-pass2edit

このニュースをザックリ言うと･･･

- 2023年8月、中国の大学研究者により、あるパスワードから文字を入れ替えたりした程度のパスワードを比較的高い精度で推測する手法についての論文が発表されています。

- 既に全く同じパスワードを複数のサービスで使い回すことは「パスワードリスト攻撃」による連鎖的な不正ログインに繋がり得ることが知られていますが、論文で参照されている調査結果によれば、あるパスワードをベースに文字を入れ替えたり追加・削除したりする等の「微調整」を行ったパスワードをサービス毎に使用するやり方をユーザーの21～33%が行っているとされています。

- 今回発表された「Pass2Edit」と呼ばれる手法では、過去に流出した約48億個のパスワードをデータセットとし、微調整されたパスワードに対する最大100回の推測実験を行ったところ、一般ユーザーが設定したものに対しては平均24.18%、セキュリティーに精通したユーザーのものに対しても11.68%が成功したとしています。

- さらに推測回数を最大1000回とした場合には、一般ユーザー・セキュリティーに精通したユーザーそれぞれに対する成功率は30.34%・15.32%に上昇したとのことです。

AUS便りからの所感等

- 論文で挙げられている、推測に成功したパスワードの微調整の例としては、「1～3文字挿入・削除」「大文字小文字の切り替え」程度にとどまらず「a⇔@」「!2#⇔123」といった文字替えや「電話番号から数字部分のみ抽出」等、及びこれらの複数のパターンの組合せを含むものが挙げられています。

- サービス毎に設定するパスワードの作り方として、ベースとなるパスワードから数文字変えて使用することを推奨するケースは少なからずみられていますが、この手法が本格的に使われた場合、全く同じパスワードでなかったとしても、連鎖的な不正ログインの被害を受ける可能性が出てくるでしょう。

- 可能な限り、パスワード管理ツール等によりランダムなパスワードをサービス毎に生成することや、多要素認証やパスキーを用いた認証を設定することが、今後さらに強く推奨されるとみられます。

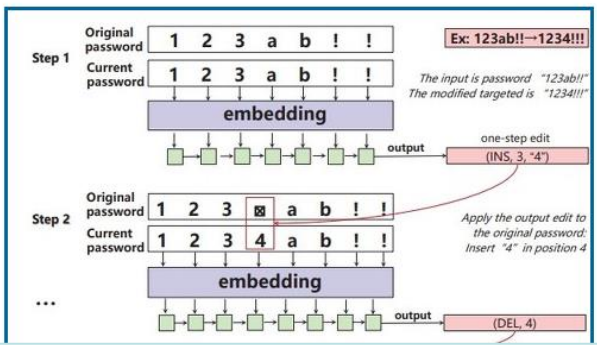
ITmedia NEWS

Innovative Tech

パスワードを“ちょっと変える”はどれくらい危ない？「abc123」→「123abc」など　中国チームが発表

2023年09月21日 08時00分 公開　[山下裕毅，ITmedia]

中国の南開大学や北京大学などに所属する研究者らが発表した論文「Pass2Edit: A Multi-Step Generative Model for Guessing Edited Passwords」は、1つのサービスで使っているパスワードを少し変えて別のサービスで使い回しているパスワードを予測して特定する攻撃を提案した研究報告である。



● 9月はWordPressの25のプラグインに脆弱性…Sucuri社発表

https://news.mynavi.jp/techplus/article/20231002-2781740/
https://blog.sucuri.net/2023/09/wordpress-vulnerability-patch-roundup-september-2023.html

このニュースをザックリ言うと･･･

- 9月28日(現地時間)、WordPress用セキュリティプラグイン等を提供する米Sucuri社より、9月に報告された25のWordPressプラグインに存在する脆弱性のまとめ記事が発表されました。

- 特に危険なものである「緊急(Critical)」レベルの脆弱性はありませんが、これに次ぐ「重要(High)」レベルの脆弱性が8件報告されており、また脆弱性の種類別ではSQLインジェクションが2件、クロスサイトスクリプティング(XSS)が5件等とされています。

AUS便りからの所感

- WordPressにおいては、提供されるプラグインも、またそれらで報告される脆弱性も数多く存在しており、Sucuri社による月毎のまとめでは、毎月20件台の報告がまとめられています。

- またWordPress本体においても不定期にセキュリティアップデートがリリースされる場合があるため、インストールした状態のままで放置するようなことは決してせず、随時本体・プラグインを最新に保つよう努めること、セキュリティを強化する何らかのプラグインを導入すること、並行して(もしくは本体・プラグインのアップデートが困難な場合を鑑みて)WAFや、IDS・IPSの導入を検討することを強く推奨致します。

SUCURI

WordPress Vulnerability & Patch Roundup September 2023

CESAR ANJOS
September 28, 2023

Vulnerability reports and responsible disclosures are essential for website security awareness and education. Automated attacks targeting known software vulnerabilities are one of the leading causes of website compromises.

To help educate website owners on emerging threats to their environments, we've compiled a list of important security updates and vulnerability patches for the WordPress ecosystem this past month.

The vulnerabilities listed below are virtually patched by the Sucuri Firewall and existing clients are protected. If you don't have it installed yet, you can use our web application firewall to protect against known vulnerabilities.

●VP8動画の処理における脆弱性報告、各ブラウザーが緊急アップデート

https://forest.watch.impress.co.jp/docs/news/1534946.html
https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_27.html
https://forest.watch.impress.co.jp/docs/news/1535316.html
https://forest.watch.impress.co.jp/docs/news/1535748.html

このニュースをザックリ言うと･･･

- 9月27日(現地時間)、米Googleより、同社開発のChromeブラウザーのセキュリティアップデート117.0.5938.132がリリースされました(10/4現在の最新バージョンは117.0.5938.150です)。

- 対応された複数の脆弱性のうち、VP8動画フォーマットの処理における脆弱性(CVE-2023-5217)はChrome自体ではなくlibvpxライブラリに存在するとされ、Chrome以外のWebブラウザーやツールにも影響するとされています。

- 9月28日にはFirefox 118.0.1、同29日にはEdge 117.0.2045.47がリリースされ、それぞれ当該脆弱性を含む複数の脆弱性に対応しており、いずれもアップデートが強く推奨されています。

AUS便りからの所感

- VP8はYouTube等で利用されていた動画フォーマットで、攻撃者が悪意のあるWebページやメール・メッセージ等から不正なVP8動画を再生させるよう誘導する、などの攻撃シナリオが考えられます。

- VP8を画像フォーマットに応用したWebPについても9月前半に脆弱性(CVE-2023-4863)が指摘され、Chrome・Firefox・Edge等でセキュリティアップデートがリリースされたばかり(AUS便り 2023/09/20号参照)。

- VP8は既に後継のVP9やAV-1に取って代わられていますが、libvpxにおけるVP9の処理にも脆弱性が存在するとの情報があり、各ブラウザー等に影響する可能性、これによるさらなるアップデートが行われる可能性がありますので、ブラウザー等が最新バージョンとなっているか随時確認することが重要です。

Impress Watch

「Google Chrome」で攻撃を確認、セキュリティアップデートがリリース
10件の脆弱性に対処。バージョンがv117.0.5938.132になっているか確認を
樽井 秀人　2023年9月28日 08:05

米Googleは9月27日（現地時間）、デスクトップ向け「Google Chrome」の安定（Stable）版をアップデートした。Windows/Mac/Linux環境にv117.0.5938.132が順次展開される。

今回のリリースは、10件の脆弱性を修正したセキュリティアップデート。CVE番号が公表されているのは以下の3件で、深刻度はいずれも「High」と評価されている。

- **CVE-2023-5217**：「libvpx」ライブラリにおけるVP8エンコーディングのバッファーオーバーフロー
- **CVE-2023-5186**：パスワード機能における解放後メモリ利用（Use after free）
- **CVE-2023-5187**：拡張機能における解放後メモリ利用（Use after free）