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。

●7月はWordPressの36のプラグインに脆弱性…Sucuri社等が注意喚起

https://news.mynavi.jp/techplus/article/20230731-2738598/
https://blog.sucuri.net/2023/07/wordpress-vulnerability-patch-roundup-july-2023.html
https://news.mynavi.jp/techplus/article/20230729-2737379/
https://patchstack.com/articles/multiple-high-severity-vulnerabilities-in-ninja-forms-plugin/

このニュースをザックリ言うと・・・

- 7月29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、7月に報告された36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。

- うち、フォーム設置用で人気のある「Ninja Forms」を含む7つのプラグインにおける脆弱性が、特に危険なものとされています。

- Sucuri社では、リスク軽減のためプラグインのアップデート等の対策を行うこと、もしくはアップデートできない場合は各種脆弱性に対応済みとされる同社提供のWAFサービスの採用を推奨しています。

- Ninja Formsについては、同じくセキュリティプラグインを提供するPatchstack社からも7月27日に脆弱性3件(Sucuri社の記事でも言及された1件含む)について注意喚起が出されています。

AUS便りからの所感等

- 36のプラグインのうちクロスサイトスクリプティング(XSS)の脆弱性が報告されたものが26あり、さらに9つのプラグインのXSS脆弱性は各プラグインの内部で使用されている共通のライブラリに由来する脆弱性(CVE-2023-33999)となっています。

- Sucuri社からの毎月のまとめ記事によれば、4月に26、5月に24、6月に23のプラグインの脆弱性が報告されており、7月はこれよりも少々多くの脆弱性報告があった模様です(この他、WordPress本体においても5月にセキュリティアップデートがリリースされています)。

- このようにWordPressは各種プラグインにも本体にもしばしば脆弱性が報告され、セキュリティアップデートがリリースされるため、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、並行してWAFやセキュリティプラグイン、IDS・IPSの導入を検討する等が重要です。

TecHr Powered by ワイヤレスニュース

WordPressプラグイン、7月に確認された脆弱性は36個 - 悪用される前に更新を

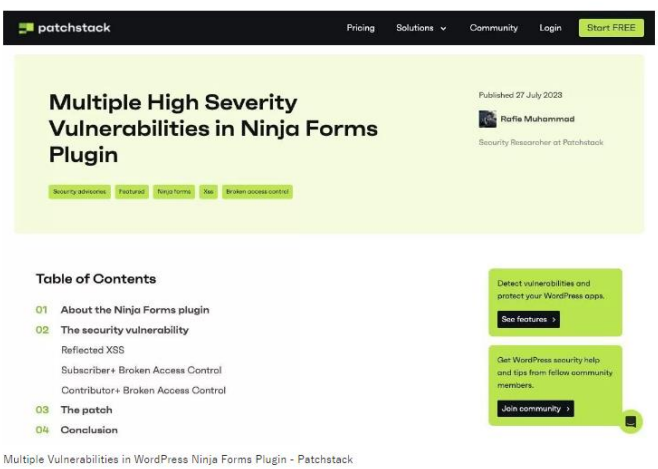
掲載日 2023/07/31 09:37　著者：後藤大地

Sucuriは7月29日(米国時間)、「WordPress Vulnerability & Patch Roundup July 2023」において、2023年7月に明らかになったWordPressのプラグインの脆弱性およびセキュリティパッチの情報について伝えた。SucuriはWebサイト所有者に対して新たな脅威を把握して対処してもらえるよう、1カ月間のWordPressエコシステムの重要なセキュリティアップデートと脆弱性パッチの一覧をまとめて公表している。

90万サイトが影響、WordPress人気のフォームプラグインに重大な脆弱性

掲載日 2023/07/29 21:05　著者：後藤大地

Patchstackは7月27日(米国時間)、「Multiple Vulnerabilities in WordPress Ninja Forms Plugin - Patchstack」において、WordPressの人気プラグインである「Ninja Forms」に複数の深刻な脆弱性があることを伝えた。90万以上のサイトに影響を及ぼす重大な脆弱性とされており注意が必要。



●Microsoft SQL Serverに不正ログインして拡散するランサムウェア「Mallox」に注意喚起

https://news.mynavi.jp/techplus/article/20230723-2732059/
https://unit42.paloaltonetworks.jp/mallox-ransomware/

このニュースをザックリ言うと･･･

- 7月20日(現地時間)、セキュリティベンダーの米Palo Alto Networks社より、Microsoft SQL Serverに侵入して拡散するランサムウェア「Mallox」の活動が活発化しているとして注意喚起が出されています。

- Malloxは2021年6月に初めて存在が確認され、SQL Serverに対しブルートフォース攻撃による不正ログインを試み、データの窃取と暗号化および身代金の要求(「支払わなければ元のデータを暴露する」という、いわゆる「二重の脅迫」)を行うとされています。

- 発表によれば、2023年前半におけるMalloxの活動が2022年後半に比べ約174%増加したことが確認されたとしています。

AUS便りからの所感

- MalloxはSQL Serverへの侵入後に外部から不正コードのダウンロードを行い、データ暗号化の前にサーバーOS上の各種管理ツール等を実行できないようにすることにより、データの復元を困難にする挙動が確認されている模様です。

- 過去にはIoTマルウェア「Mirai」についてもSQL Serverをターゲットとした亜種「BKDR_MIRAIA」が確認されています。

- SQL Serverのサービスポート(TCPポート1433番・UDPポート1434番等)に外部から直接アクセスされたり、また侵入したマルウェアがサーバーホストから外部のホストに接続したりしないよう、サーバー自身やUTMのパケットフィルタリング機能等を有効にすること、またSQL Serverで使用するユーザーアカウントについて十分に複雑なパスワードを設定するとともに、IDS・IPSの導入による不審なログイン試行の検知・遮断も検討すべきでしょう。

TECH+ Powered by マイナビニュース

Microsoft SQL Server経由で侵入するランサムウェアが増加、要注意

掲載日 2023/07/23 16:02　　著者：後藤大地

Palo Alto Networksは7月20日（米国時間）、「Threat Group Assessment: Mallox Ransomware」においてMicrosoft Windowsを標的とするMalloxランサムウェアの活動が増加しているとして、注意を呼び掛けた。

●PCからスマートフォンへの移行進む、パスワードの安全な文字数「11文字以上」の割合減少…認証方法に関するアンケート

https://www.antiphishing.jp/report/wg/authentication_20230721.html

このニュースをザックリ言うと･･･

- 7月21日(日本時間)、フィッシング対策協議会より、インターネットサービスへログインするための利用者認証に関するアンケート(2022年12月7日～12日調査、回答者533人)の結果が発表されました。

- 同協議会は2020年2月～3月にも同様のアンケート調査を実施しており(AUS便り 2020/10/05号参照)、今回の調査を新型コロナウイルス感染症・2020年東京オリンピック開催等を経たインターネット利用の状況変化に対する追跡調査と位置付けています。

- 2020年の調査から大きく変動があった事項では、インターネットサービスを利用する機器としてのPCの利用率が66.2%→40.7%と減少しており(一方Androidスマートフォンが46.6%→54.4%と増加)、スマートフォン内で完結するケース、スマートフォン利用だけを想定したサービスの増加によるものと推測されています。

- またパスワードの設定に関する設問では、「適当と思う文字数」に対し、8文字が46.6%→52.9%に比べ、10文字が16.9%→15.8%、11文字以上に至っては29.9%→10.2%と大きく減少、また「サービスによって使い分けているか」に対しては「一つを使い回している」という回答が17.4%→28.1%と増加しています。

AUS便りからの所感

- パスワードの「適当と思う文字数」については、多要素認証が増え、最初のパスワード認証については多少緩くしても良いと考えている可能性があると、また「サービスによって使い分けているか」については、多くのサービスを利用するようになったことで、利便性から使い回しの機会が増えたとそれぞれ考察されています。

- 一方で「安全性を重視したサービスと、便利な利用を重視したサービスでは、どちらを利用したいと思いますか」という設問には、前者58.0%→68.9%、後者39.5%→28.5%と前者の割合が増加している、といった結果も出ています。

- 今後、パスワードに代わる新たな認証方法とされる「Passkey」が普及すること、特にスマートフォンに慣れた世代の利用者がこれを早く受け入れる可能性があり、サービス管理者側においても情報収集を行う等して、認証方法の変化に向き合うことが求められると予想されます。

フィッシング対策協議会 Council of Anti-Phishing Japan

インターネットサービス利用者に対する「認証方法」に関するアンケート調査 コロナ禍を経た利用者の変化について、追跡調査結果を公開(2023/07/21)

2023年07月21日

フィッシング対策協議会（東京都中央区、会長：岡村久道）の認証方法調査・推進ワーキンググループ（主査：長谷部 一泰）は、フィッシング対策と関連の高いインターネットサービスの利用者認証についての 2020 年に実施した利用者へアンケート調査の追跡調査を行い、その調査結果を報告書として公開しました。

本調査は、新型コロナ感染や 2020 年東京オリンピック・パラリンピック競技大会開催などを経てインターネット利用の状況も変化しており、利用者の状況や意識にどの様な変化があったのか、 2020 年の調査をもとに追跡調査を実施しました。具体的には、フィッシング詐欺に対して日頃からどのような考えを持っているか、リスク意識、当事者意識などしっかり醸成されているか、実際としてどのようなアクションをしているかなどを調査しています。