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。

●WordPressプラグイン「LiteSpeed Cache」に致命的な脆弱性…500万以上のWebサイトに影響の恐れ

https://news.mynavi.jp/techplus/article/20240824-3010149/
https://gigazine.net/news/20240823-wordpress-litespeed-cache-plugin-vulnerability/
https://www.wordfence.com/blog/2024/08/over-5000000-site-owners-affected-by-critical-privilege-escalation-vulnerability-patched-in-litespeed-cache-plugin/

このニュースをザックリ言うと･･･

- 8月21日(現地時間)、WordPress向けセキュリティプラグイン「Wordfence」を提供するDefiant社より、WordPressのサイト高速化機能を提供するプラグイン「LiteSpeed Cache」に脆弱性(CVE-2024-28000)が存在するとして注意喚起が出されています。

- 脆弱性はLiteSpeed Cacheのバージョン6.3.0.1以前に存在し、外部の攻撃者に管理者権限を奪取され、最悪の場合サイトの乗っ取りに繋がり得るとされています。

- 既に脆弱性を修正したバージョン6.4がリリースされており、アップデートが強く推奨されています(8/29時点の最新バージョン6.4.1でもさらなるセキュリティアップデートが行われている模様です)。

AUS便りからの所感等

- LiteSpeed CacheはWebサーバー「LiteSpeed」と同じ開発元の提供で、LiteSpeed(商用版)あるいはOpenLiteSpeed(オープンソース版)上のWordPress向けの独自の高速化機能の他、Apache・nginx等といった他のWebサーバーでも動作する高速化機能も提供し、500万以上のアクティブなWordPressサイトで利用されているとのことです。

- 脆弱性の悪用により、攻撃者がWordPressサイトのユーザーとしてログインできない場合でも、ブルートフォース(総当たり攻撃)を行い、管理者ユーザーを不正に作成することが可能とされています。

- WordPressでは、本体からサードパーティー製のプラグインに至るまで日々何らかの脆弱性が報告されており、インストールしているプラグイン全てについて管理画面から更新情報を確認しつつ、最新バージョンに保つよう留意すること、またWordfence等セキュリティ機能を提供するプラグインについても、数多く提供されているものから選択の上、必ず導入することが重要です。

TECH Powered by マイナビニュース

LiteSpeed Cacheプラグインに緊急の脆弱性、500万超のWebサイトに影響

掲載日 2024/08/24 17:31　　著者：後藤大地

Defiantは8月21日(米国時間)、「Over 5,000,000 Site Owners Affected by Critical Privilege Escalation Vulnerability Patched in LiteSpeed Cache Plugin」において、WordPressの人気のプラグイン「LiteSpeed Cache」に緊急(Critical)の脆弱性が存在すると報じた。この脆弱性を悪用されると、リモートの認証されていない攻撃者にWebサイトを乗っ取られる可能性がある。

●バッファロー製のWi-Fiルーター等に脆弱性…5月にボット感染が確認、ファームウェア更新確認を

https://news.mynavi.jp/techplus/article/20240826-3012352/
https://jvn.jp/jp/JVN12824024/
https://www.buffalo.jp/news/detail/20240719-01.html
https://internet.watch.impress.co.jp/docs/news/1593570.html

このニュースをザックリ言うと･･･

- 8月23日(日本時間)、IPA・JPCERT/CCが運営する脆弱性情報サイト「JVN」より、バッファロー社製Wi-Fiルーターおよび無線LAN中継器計18機種に脆弱性(CVE-2024-44072)が存在するとして注意喚起が出されています。
- 脆弱性の悪用により、管理画面へのログイン可能な攻撃者に任意のOSコマンドをルーター上で実行される等、ルーターの乗っ取りが可能とされています。
- 5月下旬に情報通信研究機構(NICT)より、該当機器の一部にボットへの感染が確認されたとX(旧・Twitter)で発表があり、今回問題となった脆弱性を悪用して侵入されたとみられています。
- バッファロー社でもNICTと連携しての調査を行う等、経過を度々報告しており、7月までに、脆弱性が報告された全ての機種についてファームウェアのアップデートを提供済みです。

AUS便りからの所感

- 各機種へのファームウェアの自動更新は遅くとも7月22日までに開始されている模様ですが、一方で同社からは、ファームウェアの更新以外にも、「可能な限り設定を初期化し再設定する(もしくは少なくとも機器を再起動する)」「管理画面へのパスワードを推測されにくい複雑なものにする」よう呼び掛けています。
- 今回は当てはまらなかったものの、サポート切れとなった機種に脆弱性が見つかり、ファームウェア更新の提供予定はないというケースも珍しくないため、組織内で使用している機器をすべて管理下に置き、サポート切れの機器については確実にリプレースできるような体制を必ず用意しましょう。

●海外委託コンサルの私用PCにDBアクセス情報、医療従事者73万人分の個人情報流出

https://www.itmedia.co.jp/news/articles/2408/28/news196.html
https://www.sanofi.co.jp/assets/dot-jp/pressreleases/2024/240828.pdf

このニュースをザックリ言うと･･･

- 8月28日(日本時間)、フランス製薬会社の日本法人サノフィ社(以下・同社)より、同社の社内データベースが不正アクセスを受け、個人情報が流出したと発表されました。
- 被害を受けたとされるのは、医療従事者733,820人分の氏名・性別・生年月日・メールアドレス・所属医療機関等、および同社従業員(派遣・委託先含む)1,390人分の氏名とされています。
- 不正アクセスは7月10日～14日にかけて発生しており、同社が業務を委託した海外コンサルタント(以下・委託先)のノートPCがマルウェアに感染したことが原因としています。

AUS便りからの所感

- 業者は同社のセキュリティポリシーに反し、私用のノートPCにデータベースへのアクセス情報を保存していたとのことです。
- 同社では今回の事案を受けての再発防止策として、データベースアカウント管理方法の見直しや、ネットワークアクセスの制限(同社ネットワーク以外からのアクセス禁止・IPフィルタリング実施)等を発表しています。
- 「誰かがセキュリティポリシーに違反する運用をした」「個々のセキュリティ対策の1つが突破された」といったことがすぐさま無制限な侵入を許すことに繋がらないシステムであることが重要であり、また例えばネットワークアクセスの制限においても、UTM等を用いてネットワークの適宜分割・隔離等を行い、外部業者やVPNを経由してアクセスする者等について限定的なアクセスが許可できる等柔軟な設定が可能となるシステム構成等を検討すべきでしょう。