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。

●不正アクセスでフォーム改ざん…ECサイトから個人情報92,685人分・クレカ情報52,958件流出か

https://www.itmedia.co.jp/news/articles/2410/03/news164.html
https://www.tullys.co.jp/information/2024/10/post-14.html
https://togetter.com/li/2445560

このニュースをザックリ言うと･･･

- 10月3日(日本時間)、コーヒーショップチェーンを運営するタリーズコーヒージャパン社より、同社ECサイト「タリーズ オンラインストア」が不正アクセスを受け、個人情報・クレジットカード情報が流出していた可能性があると発表されました。

- 被害を受けたとされるのは、2021年7月20日～2024年5月20日に同ストアに会員登録した92,685人分の個人情報(氏名・住所・電話番号・性別・生年月日・メールアドレス・ログインID・パスワード・配送先情報)および同時期に決済で使用された52,958件のクレジットカード情報(カード番号・名義人名・有効期限・セキュリティコード)とのことです。

- 5月20日に警視庁からカード情報漏えいの可能性があると連絡を受け同日に決済を停止、23日にサイト自体の閉鎖、30日に第一報を発表していました。

- 流出の原因として、「システムの一部の脆弱性をついたことによる第三者の不正アクセスにより、ペイメントアプリケーションの改ざんが行われたため」としています。

AUS便りからの所感等

- 当該サイトは後日改修の上再開予定としており、また楽天市場上のストア、スマホアプリ等は影響は受けていないとしています。

- X(旧Twitter)上では当該サイトが改ざんされていた時点のInternet Archiveが取り上げられ、Webサイト上のスクリプトに不正なコードが難読化、付加されていた様子が指摘されています。

- 同様の事例の多くでサーバーあるいはWebサイトに侵入されて不正なファイルが設置されるケースがあるとのことで、ECサイトを構築するソフトウェアについて随時最新バージョンへのアップデートを行う、サイトを管理するアカウントに不正ログインされないため十分に強力なパスワードを設定する(可能であれば多要素認証等の採用も検討する)、またWebサイト上に脆弱性等がないか第三者による診断を受ける等を強く推奨致します。

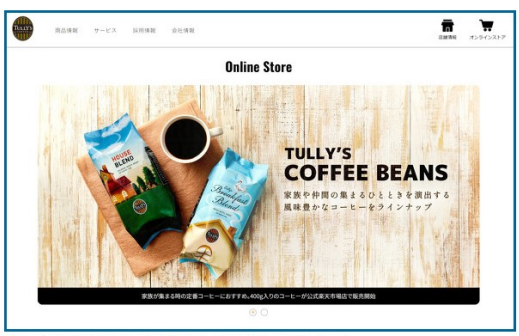
ITmedia NEWS

「タリーズ オンラインストア」クレカ情報5万件流出、IDやパスワードなど9万件も　ペイメントアプリ改ざんで

2024年10月03日 17時11分 公開　[ITmedia]

タリーズコーヒージャパンは10月3日、直営の通販サイト「タリーズ オンラインストア」が不正アクセスを受けてペイメントアプリが改ざんされ、ユーザーのIDやパスワード9万2685件が流出した可能性があると発表した。

うち、クレジットカード番号を登録していたユーザー5万2958件は、カード番号やセキュリティコードなども流出したおそれがあるという。



タリーズ オンラインストア（現在は休止中。楽天市場店のみ運営している）

●Microsoft月例のセキュリティアップデートリリース、Win11 22H2からはバージョンアップを

https://forest.watch.impress.co.jp/docs/news/1629891.html
https://msrc.microsoft.com/blog/2024/10/202410-security-update/

このニュースをザックリ言うと・・・

- 10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 KB5044273(ビルド 19045.5011)、11 23H2 KB5044285(ビルド 22631.4317)および11 24H2 KB5044284(ビルド 26100.2033)となります。

- なお、Windows 11 22H2については、今回のアップデートでサポートが打ち切られるため、23H2または24H2へバージョンアップするよう呼び掛けられています。

AUS便りからの所感

- この他Adobe社各製品についても同9日に月例アップデートがリリースされていますが、Acrobat Readerは先んじて同4日に24.003.20180がリリースされています。

- また同16日にはOracleからもJavaやMySQL等に対する4半期毎のセキュリティアップデートがリリース予定です。

- MSをはじめとする各社からのセキュリティアップデート発表が集中する第2水曜日(日本時間。1日が水曜日の場合は第3水曜日)等、運用している各種プロダクトについて定期的なアップデートのスケジュールが定まっているものを把握し、またアップデートの適用までに未修正の脆弱性に対し発生し得る攻撃に対しアンチウイルス・UTM等による防御策をとることが肝要です。

Impress Watch

Microsoft、2024年10月セキュリティ更新を公開 ～「バージョン 24H2」は初のパッチ

ゼロデイを含む117件の問題へ新たに対処

樽井 秀人　2024年10月9日 09:05

2024年10月のセキュリティ更新プログラム

米Microsoftは10月8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117件（サードパーティーのものも含めれば121件）の脆弱性が新たに対処されている。

●Linuxに感染するマルウェア「perfctl」に注意喚起、数千台のサーバーに侵入か

https://gigazine.net/news/20241007-perfctl-malware-linux/
https://www.aquasec.com/blog/perfctl-a-stealthy-malware-targeting-millions-of-linux-servers/

このニュースをザックリ言うと・・・

- 10月3日(現地時間)、セキュリティベンダーのAqua Security社より、Linuxに感染し暗号資産(仮想通貨)Moneroのマイニング等を行うマルウェア「perfctl」に関する注意喚起が出されています。

- 同社の分析によれば、perfctlはサーバーの設定上の問題を突いて侵入、2022年に発見されたLinuxのソフトウェアPolkitの脆弱性(AUS便り2022/02/01号参照)を悪用してroot権限の奪取を図り、ルートキットによる秘匿化を行う、外部との通信にTorによる暗号化通信を用う、ユーザーがログインしていない時にのみマイニングを行う等、巧妙に監視を逃れる行動をとっているとのことです。

- 同社ではperfctlが3年以上前から活動しているとみており、数百万台のサーバーが攻撃を受け、うち数千台に侵入されていると分析しています。

AUS便りからの所感

- perfctlはサーバーに侵入後、「/usr/bin」ディレクトリに「perfcc」「wizmlsh」ファイルや「.local(先頭にドットがつく隠しディレクトリ)」ディレクトリを作成する他、「/tmp」「/usr/lib」「/root」等にも不審なファイル・ディレクトリを作成するとしています。

- Aqua社ではperfctlの検出方法として、こういった場所に不審なファイルが作成されていないか確認すること等を挙げています(正常なファイルを間違えて削除しないこと、一方で通常のOSの設定ファイル等についてperfctlが改変している可能性もあることに注意が必要です)。

- 他にもperfctlが通信するとされる特定のIPアドレスへの通信、CPU使用率が不自然に上昇していることがないか、本来ありえない場所に置かれている「httpd」「sh」等が実行されていないか、等の監視も挙げられています。

- ともあれLinux上で実行されるマルウェアも存在し、サーバーに侵入する可能性があることを認識し、Windows等と同様にアンチウイルスやUTMによる保護を可能な限り行うべきです。

GIGAZINE

2024年10月07日 13時26分　セキュリティ

勝手にCPUを100%使って仮想通貨をマイニングするLinux向けマルウェア「perfctl」が発見される、ログイン時は活動を停止するので発見困難で数百万台のサーバーが標的になった可能性

「perfctl」と呼ばれるLinux向けマルウェアが3年以上前から活動していたことが明らかになりました。perfctlはCPUを100%使って仮想通貨「Monero」をマイニングするマルウェアで、数百万台のサーバーが標的となり数千台のサーバーが実際に被害を受けたと推測されています。