

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。

●問い合わせフォームが設置できるWebアプリケーションに脆弱性…個人情報漏洩の恐れ

<https://www.itmedia.co.jp/news/articles/2304/17/news154.html>

<https://iubei.co.jp/formmail/info20230414.html>



このニュースをザックリ言うと…

- 4月14日(日本時間)、ソフトウェア開発等の業務を行っているジューベ社より、同社が配布しているWebアプリケーション「JB問い合わせフォーム」に脆弱性が存在すると発表され、最新バージョン0.7.0がリリースされています。

- 脆弱性は同ソフトウェアのバージョン0.40~0.6.1に存在し、悪用により、保存された問い合わせ内容が外部から閲覧可能とされ、個人情報漏洩に繋がりが得るものとなっていました。

- 同社では速やかにバージョン0.7.0へのアップデートを行うこと、もしくは回避策として、プログラムファイルや、問い合わせ内容が保存されるデータファイルの削除を呼び掛けています。

AUS便りからの所感等

- 2000年前後において、外部から直接アクセス可能なドキュメント領域下に個人情報を含むCSVファイル等が保存されているのが多数のWebサイトで発見され、アングラ系の掲示板等で相次いで暴露される事例がありました。

- JB問い合わせフォームも、設置したディレクトリ下に作成されるデータ用ディレクトリ内のファイルに問い合わせ内容を保存する仕組みをとっていましたが、当該ディレクトリに直接アクセスできないためのApache用設定ファイルが同梱されており、アプリケーションに対する不正なリクエストで脆弱性を悪用することによるデータファイルへの不正アクセスが可能だったと推測されます。

- Webサーバーにファイルをアップロードする形でインストールされたアプリケーションについては、概ね自動更新やその通知機能がないと考えられるため、最新バージョンのリリース時には早急にアップデート対応ができるよう把握・管理しておくこと、またインストール時のファイルのパーミッション設定については、単にWebサーバーから書き込み可能だけでなく、不必要な読み書き設定がないか等にも十分に注意を払ってください。



“問い合わせフォーム作成キット”に脆弱性 入力内容を第三者が取得できる状態に

© 2023年04月17日 17時20分 公開

[ITmedia]

ソフトウェア開発を手掛けるジューベ（東京都足立区）は4月14日、同社が配布している「JBお問合せフォーム」のプログラムに情報漏えいの脆弱性があったとして謝罪した。送信内容を第三者が閲覧できる状態だったという。

■ Jubei サービス開発 Webシステム 事業内容

トップ / JB問い合わせフォーム / 設置方法

設置方法

PHPに対応したレンタルサーバー等で動作します。

- zipファイルをダウンロード、展開する
当サイトで配布しているzipファイルをダウンロードし、展開してください。
- レンタルサーバーにアップロードする
WinSCPなどのソフトを用いて、レンタルサーバーにアップロードします。

WinSCP

ファイル式選択後

●ゴールデンウィークにおけるセキュリティ面の注意喚起、IPA・経産省等から発表

<https://www.ipa.go.jp/security/anshin/heads-up/alert20230420.html>
<https://www.meti.go.jp/press/2023/04/20230424002/20230424002.html>

このニュースをザックリ言うと…

- 4月20日(日本時間)、IPAより、「**ゴールデンウィークにおける情報セキュリティに関する注意喚起**」が発表されました。
- GW等**長期休暇の時期**、企業・組織によっては、「**システム管理者が長期間不在になる**」「**友人や家族と旅行に出かける**」等、**いつもとは違う状況**になり、ウイルス感染・不正アクセス等の被害発生時の対処が遅れる、あるいはSNSへの書き込み内容から思わぬ被害が発生する等の可能性があることを鑑み、「**企業や組織の管理者**」「**企業や組織の利用者**」「**個人の利用者**」それぞれを対象に、「**休暇前**」「**休暇中**」「**休暇明け**」に行うべき**基本的な対策と心得**が「**長期休暇における情報セキュリティ対策**」においてまとめられています。
- 同24日には、**経済産業省・総務省・警察庁および内閣官房内閣サイバーセキュリティセンター(NISC)**からも、「**春の大型連休において実施いただきたい対策について**」の注意喚起が**連名**で出されています。

AUS便りからの所感

- それぞれの発表は**2022~2023年の年末年始の時などと大きく異なるようなものではなく**、経産省等の発表では管理者に向けて、**休暇前の「対処手順・連絡体制」「バックアップ」**について特に注意するよう呼び掛けています。
- IPAでは**ランサムウェアによるサイバー攻撃**に関する相談、特に**リモートデスクトップサービス(RDP)**や**VPN装置**への侵入の事例が多く寄せられているとしています。
- GWまでに日にちがなく十分な対応が間に合わなかったとしても、**GW明け以降に点検すべきことは多く存在しますし、以後も夏季休暇等に備えて対応しておくべき事柄も変わらず、また長期休暇に関係なく常時から注意すべき普遍的なものも「日常的に実施すべき情報セキュリティ対策」**(<https://www.ipa.go.jp/security/anshin/asures/everyday.html>)として別途まとまっており、それぞれにおいて準備・点検を行うよう意識していくことが肝要です。



ゴールデンウィークにおける情報セキュリティに関する注意喚起

資料更新日：2023年4月25日
独立行政法人情報処理推進機構
セキュリティセンター

多くの人がゴールデンウィークの長期休暇を取得する時期を迎えるにあたり、IPAが公開している長期休暇における情報セキュリティ対策をご案内します。

長期休暇の時期は、「システム管理者が長期間不在になる」、「友人や家族と旅行に出かける」等、いつもとは違う状況になります。このような場合、ウイルス感染や不正アクセス等の被害が発生した場合に適切な対応が遅れたり、SNSへの書き込み内容から思わぬ被害が発生したり、場合によっては関係者に対して被害が及ぶ可能性があります。

このような事態をならぬよう、(1)企業や組織の管理者、(2)企業や組織の利用者、(3)個人の利用者、のそれぞれの対象者に対して取るべき対策をまとめています。

長期休暇における情報セキュリティ対策

また、長期休暇に限らず、日常的に行うべき情報セキュリティ対策も公開しています。

日常的な情報セキュリティ対策

被害に遭わないためにもこれらの対策の実施をお願いします。

政府からも長期休暇に向けた注意喚起が行われていますので、あわせてご確認ください。

春の大型連休において実施いただきたい対策について注意喚起を行います



●Chromeに致命的な脆弱性とセキュリティアップデート相次ぐ… 112.0.5615.138への更新確認を

<https://gigazine.net/news/20230417-google-chrome-emergency-update-exploited-zero-day/>
https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_14.html
https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html

このニュースをザックリ言うと…

- Google社開発の**Chromeブラウザ**において、**致命的な脆弱性に対するセキュリティアップデートが相次いでリリース**されています。
- **4月14日**(現地時間)、ChromeのJavaScriptエンジンにて既に攻撃が確認されていた(いわゆる**ゼロデイ脆弱性**)「**CVE-2023-2033**」等2件の脆弱性を修正した**緊急のセキュリティアップデート112.0.5615.121**が**リリース**されています。
- **同18日**には、やはりゼロデイ脆弱性とされる「**CVE-2023-2136**」含む**5件を修正した112.0.5615.138**が**リリース**されています。

AUS便りからの所感

- 4/25現在、**Edgeブラウザ**でも**109.0.1518.100**がリリースされ、**Chromeと同じエンジンを使用する他のブラウザ**でも**同様のセキュリティアップデートがリリース**されています。
- CVE-2023-2136は**Linux・Android・macOS**に影響するグラフィックライブラリーの脆弱性で、**Windowsには影響しません**が、112.0.5615.138は他にも複数の脆弱性が修正されており、**アップデートは必要不可欠**です。
- Chromeでは**アップデートの適用後に再起動を促すメッセージが表示**されますが、リリースから適用・メッセージの表示まで**タイムラグが発生する場合があります**ため、「ヘルプ」→「Google Chromeについて」(もしくはchrome://settings/help)にて、**最新バージョンへ確実にアップデートされているか確認**する習慣をつけることが肝要です。



2023年04月17日 10時51分

セキュリティ

ChromeのV8 JavaScriptエンジンのゼロデイ脆弱性に対する緊急アップデートをGoogleが実施、既に攻撃に悪用されまくっているため

Googleが2023年4月14日に、Google Chromeの**ゼロデイ脆弱(ぜいじゃく)**性に関する緊急アップデートをリリースしました。Googleはこのアップデートにより、深刻度が「高」と設定された脆弱性の「**CVE-2023-2033**」に対応しました。

