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。

●Reactに重大な脆弱性、Next.js等にも影響…至急アップデートを

https://www.jpcert.or.jp/newsflash/2025120501.html
https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components
https://nextjs.org/blog/CVE-2025-66478

このニュースをザックリ言うと・・・

- 12月3日(現地時間)、JavaScriptライブラリー「React(React.js)」開発元より、Reactに脆弱性「CVE-2025-55182」が存在することが発表され、セキュリティアップデートがリリースされています。

- 脆弱性はReactのサーバー側で稼働するコンポーネントに存在し、悪用により、Webサーバーを外部から乗っ取られる恐れがあるとしています。

- 既に脆弱性を悪用するコードや、攻撃者グループによる悪用が確認されていると言われており、バージョン19.2.1・19.1.2および19.0.1へ至急アップデートを行うよう呼び掛けられています。

- 同日、ReactをベースとするWebアプリケーションフレームワーク「Next.js」にも同様の脆弱性(CVE-2025-66478)があると発表、セキュリティアップデート(16.0.7・15.5.7他)がリリースされており、同様にReactを含んでいるソフトウェア等にも影響するとみられます。

AUS便りからの所感等

- Reactは当初クライアント側でレンダリングするWebアプリケーション向けライブラリーとして開発され、のちサーバー側でのレンダリングを行う「React Server Components(RSC)」が登場しており、脆弱性はRSCに存在しています。

- 脆弱性はWebサイトに対し不正なリクエストを送信するだけで可能とされ、Webサーバー上で任意のコマンドを実行される恐れがあるとしており、サーバー上にある機密情報の読み取り、Webサイトのコンテンツの改ざん、あるいはサーバーを踏み台としての第三者ホストへのアクセス等様々なシナリオが考えられます。

- 多くのWebサイトで利用されるソフトウェアでこのような脆弱性が存在する事例は、例えばStruts・Spring FrameworkのようなJava製のアプリケーションフレームワーク、およびそれらを稼働させるTomcatアプリケーションサーバーでも度々報告され、決済フォームの改ざんによるクレジットカード情報の流出等に繋がることも珍しくなく、Webアプリケーションでどういったソフトウェア・ライブラリーを使用しているかを把握すること、それらに対するセキュリティアップデートがリリースされ次第確実に適用すること、また脆弱性を悪用する不正なアクセスを遮断するためのWAF(Webアプリケーションファイアウォール)等の採用を検討することが重要です。


JPCERT CC
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

React Server Componentsの脆弱性（CVE-2025-55182）について
最終更新: 2025-12-05

ポスト メール
CyberNewsFlash一覧

I. 概要

2025年12月3日（現地時間）、React Server Componentsにおける認証不要のリモート コード実行の脆弱性（CVE-2025-55182）が公開されました。攻撃者が細工したHTTPリクエスト（HTTP経由の不正なFlightペイロード）をReact Server Components（RSC） を処理するサーバーに送信することで、認証不要のリモートコード実行につながる可能性が あります。

なお、JPCERT/CCでは有効な概念実証（PoC）コードの公開を確認しました。 今後本脆弱性が悪用される可能性が高まっていると考えられます。

本脆弱性の影響を受ける製品を利用している場合は、後述「III. 対策」に記載の情報を 確認の上、対策の実施を検討してください。

II. 対象

（React）
次のパッケージのバージョン19.0、19.1.0、19.1.1、19.2.0が本脆弱性の影響を受けます。

- react-server-dom-webpack
- react-server-dom-parcel
- react-server-dom-turbopack

● 2025年版「最も危険なパスワード」Nord Security発表

https://dime.jp/genre/2053699/
https://nordpass.com/most-common-passwords-list/

このニュースをザックリ言うと･･･

- 11月中旬、パスワード管理ツール「NordPass」等を提供するNord Security社より、「Top 200 most common passwords of the year 2025(2025年における最もよく使用されたパスワード トップ200)」と題したランキングが発表されました。

- 2024年9月～2025年9月に、外部のセキュリティインシデント研究者と協力の上、公的なデータ漏洩事案とダークウェブ上のデータを調査した結果とのことです。

- 1位は「123456」、以下10位まで「admin」「12345678」「123456789」「12345」「password」「Aa123456」「1234567890」「Pass@123」「admin123」となっています。

- 44の国・地域ごとのランキング(トップ20)も発表されており、日本は10位まで「admin」「123456」「password」「Freemima123」「12345678」「yamamoto2580」「Chan8899」「rosycash」「102030Abcd」「mokariku」となっています。

AUS便りからの所感

- 本ランキングは2019年以降毎年同社から発表されていますが、ほぼ毎回「123456」が1位(2019年は「12345」、2022年は「password」が1位でした)であり、「数字の羅列」「password・admin等簡単な1単語と数字の組み合わせ」「qwerty・1qaz2wsx・asdfghjkl等キーボード上で並んでいる文字列」が多数を占めている他、「ユーザー本人の名前」「趣味に関連した単語(YouTube・TikTokで活躍する有名人のハンドル等)」も目立っている模様です。

- 少なくともランキングに掲載されていたり、それ以外でも前述したようなパターンに当てはまったりするパスワードを避けるべきなのは当然ですが、「大文字・小文字・数字・記号を全て含める」等を強制すべきかについては近年疑義も示されており、複数の単語からなる(場合によっては空白で区切る)「パスフレーズ」で文字数が十分に長い(16～20文字以上)ものであれば、総当たりや辞書攻撃に対し概ね安全である、またパスワードを設定させるサービス側に対しても設定可能な最大長を16文字以内等に制限してはいけないとする意見が出ています。

- 「使い回しを避ける」「管理ツールの使用ないしそれによる複雑なパスワードの生成」等が言われてきた段階を経て、近年はパスワードだけによる認証も安全ではなく、多要素認証やパスキー等に移行すべきという論調も既に有力であり、これらの検討とともに、認証において重要や役割を担うスマートフォン等についてもマルウェアや不正なアプリが侵入しないよう十分に注意をはらうようにしてください。

● Chrome・Edgeのバックドア・スパイウェアを含む拡張機能、約430万人に被害か

https://gigazine.net/news/20251204-browser-extension-malware/
https://www.koi.ai/blog/4-million-browsers-infected-inside-shadypanda-7-year-malware-campaign

このニュースをザックリ言うと･･･

- 12月1日(現地時間)、Koi Security社より、ChromeおよびEdgeブラウザーの約430万人のユーザーが不正な拡張機能によるマルウェア感染の被害を受けていたとする調査結果が発表されました。

- 「ShadyPanda」と呼ばれる攻撃者は、まず2023年にEdge向けに125種、Chrome向けに20種の拡張機能を公式の拡張機能ストアにリリースし、インストールしたブラウザー上で、AmazonやeBay等ECサイトへのリンクにアフィリエイトコードを仕込む等の詐欺行為を行っており、次いで2024年初頭には、ユーザーの検索内容、Cookieおよび検索ボックス上でのキーストローク内容を外部に送信する拡張機能をリリースしていたとのことです。

- 2024年半ばには「Clean Master」等5種の拡張機能にバックドアのコードを含むバージョンをリリースしたとしており、それらの中には2018年以降に無害な拡張機能としてリリースされ、以降20万回以上インストールされていたものも含まれていたとしています。

- 前後して2023年にはEdge向けに「WeTab New Tab Page」等5種のスパイウェア入り拡張機能をリリースし、合わせて400万回以上と、前述した「Clean Master」を凌ぐインストール数を達成したとしています。

AUS便りからの所感

- 一連の攻撃で用いられた拡張機能は前述のように壁紙を中心としたものでしたが、Chrome・Edgeにて新しい仕様「Manifest v3」に対応しない古い拡張機能が無効化される流れが進み、更新されていない拡張機能のManifest v3対応版を騙る偽の拡張機能がアップロードされるケースも散見されています。

- 記事では公式ストア側が最初の掲載申請時のみ審査を行い、無害な拡張機能として広くインストールされてからマルウェア化する手口を検出できていないことを指摘しており、SNSでの報告等を十分に確認し、必要最低限の拡張機能のみインストール・有効化する等の自衛策をとるぐらいしかできないユーザー側に対し、公式ストアやその他のセキュリティベンダー等が、安全に拡張機能を提供できる体制を整えられるかが注目されるところです。