2025 年 12 月 17 日

報道関係各位

GMO サイバーセキュリティ by イエラエ株式会社

GMO サイバーセキュリティ by イエラエ、「GMO サイバー攻撃 ネット de 診断 ASM」で React.js の深刻な脆弱性「React2Shell」に緊急対応

～CVSS スコア 10.0、危険度最高レベルの脆弱性への早期対策を支援～

GMO インターネットグループの GMO サイバーセキュリティ by イエラエ株式会社(※1)（代表取締役 CEO：牧田 誠 以下、GMO サイバーセキュリティ by イエラエ）は、2025 年 12 月 3 日、外部公開 IT 資産を自動で棚卸し・可視化するアタックサーフェスマネジメント(※2)（Attack Surface Management、ASM）ツール「GMO サイバー攻撃 ネット de 診断 ASM」をアップデートし、JavaScript ライブラリ「React.js」に存在する深刻なリモートコード実行の脆弱性「React2Shell（CVE-2025-55182）」の検知に対応しました。

「React2Shell（CVE-2025-55182）」は、CVSS(※3) スコアが最高値の 10.0 で、すでにサイバー攻撃での悪用が確認されている非常に危険な脆弱性です。今回のアップデートにより、「GMO サイバー攻撃 ネット de 診断 ASM」の利用者は、本脆弱性を迅速に確認し、適切な対応を行うことが可能になります。

(※1)GMO サイバーセキュリティ by イエラエ株式会社は GMO インターネットグループ株式会社の連結会社です。

(※2)インターネットに公開されているサーバーやネットワーク機器など IT 資産の情報を収集・分析することにより、不正侵入経路となりうる脆弱性やそのリスクを検出・評価する取り組みのこと。

(※3)ソフトウェアやシステムの脆弱性の深刻度を評価する国際的な指標。深刻度は 0.0～10.0 の数値で表され、10.0 が最も危険度が高い。

【「React2Shell（CVE-2025-55182）」の概要と影響】

「React2Shell（CVE-2025-55182）」は、JavaScript ライブラリ「React.js」の React Server Components（RSC）に存在する、リモートコード実行の脆弱性です。攻撃者はこの脆弱性を悪用することで、対象システム上で任意のコードを実行し、完全な制御を奪う可能性があります。これにより、個人情報の窃取、システム破壊、ランサムウェア感染など、企業にとって致命的な被害をもたらす恐れがあります。また、その影響は「Next.js」など「React.js」と依存関係にあるソフトウェアにも及びます。

「React2Shell（CVE-2025-55182）」の CVSS スコアは最高値の 10.0 で、すでに実際のサイバー攻撃での悪用が確認されています。

「GMO サイバー攻撃 ネット de 診断 ASM」では、本脆弱性の脅威を極めて深刻な問題と捉え、脆弱性が発表された即日中に検知機能をアップデートしました。これにより、お客様は本脆弱性が存在するソフトウェアの利用状況を確認し、迅速な対策実施が可能となります。今後も、最新の脆弱性情報を迅速に反映し、進化するサイバー攻撃に対応するための機能強化とサポート体制の充実を継続してまいります。

【「GMO サイバー攻撃 ネット de 診断 ASM」アップデート概要】

今回のアップデートにより、以下の診断項目を追加しました。

既知の脆弱性が存在するソフトウェアの利用(React.js)	「React2Shell（CVE-2025-55182）」が報告されているバージョンを利用している場合に指摘事項として通知されます。 対策方法は本脆弱性が修正されたセキュリティパッチの適用を推奨します。 パッチを適用すること本脆弱性を悪用したサイバー攻撃の被害を未然に防ぐことができます。

【「GMO サイバー攻撃 ネット de 診断 ASM」について】
(https://product.gmo-cybersecurity.com/net-de-shindan/lp_enterprise/)

「GMO サイバー攻撃 ネット de 診断 ASM」は、簡単かつ直感的に使用が可能なセキュリティプラットフォームです。国産 ASM ツールとして培ってきた「IT 資産の棚卸しとリスク可視化」の強みを活かしながらも、ASM ツールの枠にとどまらず「複雑化するセキュリティ運用をシンプルにし、“何から対策すべきか”を可視化する」というビジョンの実現を目指しています。セキュリティ知識を問わず、お客様が最も優先すべき対策を一目で把握できるよう導きます。

【GMO サイバーセキュリティ by イエラエについて】
(https://gmo-cybersecurity.com/)

GMO サイバーセキュリティ by イエラエは、国内最大規模のホワイトハッカーで組織されたサイバーセキュリティのプロフェッショナルカンパニーです。会社理念である「人を助ける信念を守るチカラに変えていく」ために今後も最先端の技術と実践的な教育を通じて、日本のサイバーセキュリティの強化に貢献していきます。また、「世界一のホワイトハッカーの技術力を身近に」を目指して、各種脆弱性診断、ペネトレーションテスト、セキュリティコンサルタント、SOC サービス、フォレンジック調査まで包括的にサイバーセキュリティ対策サービスをご提供します。

以上

【報道関係お問い合わせ先】

●GMO サイバーセキュリティ by イエラエ株式会社
マーケティング部　広報担当　伊礼・棚田
TEL：03-6276-6045
E-mail：pr@gmo-cybersecurity.com

●GMO インターネットグループ株式会社
グループ広報部　PR チーム　田部井
TEL：03-5456-2695
お問い合わせ：https://group.gmo/contact/press-inquiries/

【GMO サイバーセキュリティ by イエラエ株式会社】（URL：https://gmo-cybersecurity.com/）

会　社　名	GMO サイバーセキュリティ by イエラエ株式会社
所　在　地	東京都渋谷区桜丘町 26 番 1 号　セルリアンタワー
代　表　者	代表取締役 CEO　牧田　誠
事 業 内 容	■Web アプリ及びスマホアプリ脆弱性診断 ■ペネトレーションテスト ■不正利用(チート)診断 ■IoT 脆弱性診断 ■自動車脆弱性診断 ■フォレンジック調査 ■CSIRT 支援 ■クラウドセキュリティ診断 ■クラウドセキュリティ・アドバイザリー
資　本　金	1 億円

【GMO インターネットグループ株式会社】（URL：https://www.group.gmo/）

会　社　名	GMO インターネットグループ株式会社　（東証プライム市場　証券コード：9449）
所　在　地	東京都渋谷区桜丘町 26 番 1 号　セルリアンタワー
代　表　者	代表取締役グループ代表　熊谷　正寿
事 業 内 容	持株会社（グループ経営機能） ■グループの事業内容 インターネットインフラ事業 インターネットセキュリティ事業 インターネット広告・メディア事業 インターネット金融事業 暗号資産事業
資　本　金	50 億円