2026 年 2 月 2 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 FortiSIEM の深刻な未認証リモートコード実行脆弱性に緊急対応

～セキュリティ監視基盤を悪用する攻撃リスクの把握と、迅速な対策判断を支援～

GMO サイバーセキュリティ by イエラエ株式会社（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）(※1)は、2026 年 1 月 29 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(※2)（Attack Surface Management、以下 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、Fortinet 社が提供するセキュリティ情報管理・イベント管理（SIEM）製品「FortiSIEM」に存在する深刻な脆弱性「CVE-2025-64155」に関する診断項目を追加しました。本脆弱性は、OS コマンドインジェクション(※3)に起因するものであり、認証を必要とせず外部から任意のコード実行（RCE）(※4)が可能となるおそれがあります。

本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、「FortiSIEM」の深刻な脆弱性（CVE-2025-64155）を早期に把握し、自組織の攻撃面におけるリスク状況の可視化、パッチ適用やネットワーク制御、監視強化など、優先度を踏まえた対策方針の検討を迅速に行うことが可能になります。

GMO サイバーセキュリティは今後も、実際の攻撃動向や悪用可能性を踏まえた ASM 機能の強化を通じて、企業・組織のサイバーリスク低減を支援してまいります。

(※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)OS コマンドインジェクションとは、システムが受け取った入力を適切に確認せず処理してしまうことで、攻撃者がサーバー上で本来想定されていない操作を実行できてしまう脆弱性のこと。

(※4)未認証のリモートコード実行（Unauthenticated Remote Code Execution / RCE）とは、認証を行わずに外部から任意のプログラムやコマンドを実行できる脆弱性のこと。

【「FortiSIEM」の未認証リモートコード実行につながる深刻な脆弱性（CVE-2025-64155)】

2026 年 1 月 13 日に公開された本脆弱性（CVE-2025-64155）は、Fortinet 社が提供するセキュリティ情報管理・イベント管理（SIEM）製品「FortiSIEM」に存在する深刻な脆弱性で、CVSS スコア(※5)も 9.8（Critical）と非常に危険性が高い脆弱性です。本脆弱性は、認証を必要とせず外部から任意のコードを実行される可能性があります。攻撃者に悪用された場合、対象システムの完全な制御を許し、システム環境や構成次第では多様な攻撃に悪用されるおそれがあります。

「FortiSIEM」は、世界で数十万を超えるビジネス顧客基盤を持つ Fortinet 社のセキュリティソリューションの中核的製品として広く利用されており、日本国内においても基幹システムの運用環境を含む多様な企業・組織での利用が進んでいます。「FortiSIEM」は、企業や組織におけるセキュリティ監視の中核を担う基盤であることから、脆弱性を悪用された場合の影響は広範に及び、事業継続に重大な影響を及ぼすことが想定されます。具体的には、以下のようなリスクが考えられます。

- ログや証跡の欠損・改ざんによる、インシデント調査や原因究明の困難化
- 証跡の欠損により、コンプライアンス対応や監査要件を満たせない期間が発生するリスク
- 原因究明や対外説明の遅延による、復旧プロセスへの影響
- 基幹システム侵害、ランサムウェア被害、情報漏えい等の二次被害

(※5)ソフトウェアやシステムに存在する「脆弱性（セキュリティ上の欠陥）」の深刻度を、0.0 から 10.0 の数値で表す国際的な標準指標

【「GMO サイバー攻撃 ネット de 診断 ASM」アップデート概要】

「GMO サイバー攻撃 ネット de 診断 ASM」では、「FortiSIEM」の深刻な脆弱性「未認証リモートコード実行につながる深刻な脆弱性（CVE-2025-64155)」への対応として、新たに以下の診断項目を追加しました。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」は、外部に公開された IT 資産の中から「FortiSIEM」の該当の脆弱性（CVE-2025-64155）が残存するバージョンの利用を検知した場合に、指摘事項および対策を通知します。これにより、利用者は自組織の攻撃面におけるリスク状況を早期に把握し、パッチ適用やネットワーク制御、監視強化など、優先度を踏まえた対策方針の検討を迅速に行うことが可能になります。

「CVE-2025-64155」の検知 (既知の脆弱性が存在する ソフトウェアの利用)	「FortiSIEM」の該当の脆弱性（CVE-2025-64155）が残存するバージョンの利用を検知した場合に、指摘事項および対策を通知します。

【「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