Cisco Secure Malware Analytics アプライアンス（旧 Threat Grid アプライアンス）バージョン 2.19 リリースノート

最終更新：2025 年 1 月 27 日

はじめに

このドキュメントでは、Cisco Secure Malware Analytics（旧 Threat Grid）アプライアンス バージョン 2.19.0 のリリース ノート、および既知の問題について説明します。

ユーザーマニュアル

入手可能な Cisco Secure Malware Analytics（旧 Threat Grid）アプライアンスのユーザーマニュアルを次に示します。

Cisco Secure Malware Analytics アプライアンスのユーザーマニュアル

アプライアンスのユーザーマニュアルは、シスコ Web サイトの Cisco Secure Malware Analytics アプライアンスのインストールとアップグレードに関するガイドのページを参照してください。

（注） 新しいドキュメントは、Cisco Secure Malware Analytics アプライアンスの製品とサポートのページから入手できます。

バックアップに関するよくある質問

技術情報と手順については、『Backup Notes and FAQ』を参照してください。

クラスタリングの概要とよくある質問

詳細については、『Clustering Overview and FAQ』を参照してください。

更新のインストール

Cisco Secure Malware Analytics（旧 Threat Grid）アプライアンスを新しいバージョンに更新する前に、シスコ Web サイトの Cisco Secure Malware Analytics アプライアンスのインストールと

アップグレードに関するガイドのページから入手できる『Appliance Setup and Configuration Guide』の説明に従って、初期設定および構成手順を完了しておく必要があります。

新しいアプライアンス：新しいアプライアンスが古いバージョンとともに出荷されていて、更新をインストールする場合は、先に初期設定を完了する必要があります。すべてのアプライアンス設定が完了するまで、更新を**適用しないでください**。

ライセンスがインストールされるまでアプライアンスの更新はダウンロードされず、アプライアンスが完全に設定されない限り（データベースを含む）、正しく適用されない可能性があります。

Cisco Secure Malware Analytics アプライアンスの更新は、管理 UI ポータルを介して適用されます。

アップデートは一方向です。より新しいバージョンにアップグレードすると、以前のバージョンに戻すことはできません。

更新をテストするには、分析用のサンプルを提出してください。

修正と更新

バージョン 2.19.6

- **タイブレーカーとしてクラスタに参加**：ノードがタイブレーカーとして参加するとインストール時にクラスタの再初期化が発生する問題を修正しました。
- **予期しないアップグレードの防止**：再起動後の予期しないアップグレードを防ぐための暫定修正。

バージョン 2.19.5

- **サポートセッション証明書**：サポートセッションの期限切れの証明書チェーンを更新する機能を追加しました。

バージョン 2.19.4

- **ポリシールーティングの強化**：ネットワークトラフィックの管理を円滑化するために、ポリシールーティングを改善しました。
- **新しいファームウェア更新ツール**： M5 および M6 世代アプライアンスに特化して設計されたファームウェア更新ツールを追加しました。この新機能の使用方法の詳細については、管理者ガイドを参照してください。

バージョン 2.19.3

このリリースでは、さまざまな修正と拡張機能が追加されています。

- http2 高速リセット攻撃に対する修正プログラムを提供するために、コンポーネントを更新しました。関連する CVE：CVE-2024-27983、CVE-2024-27919、CVE-2024-2758、CVE-2024-2653、CVE-2023-45288、CVE-2024-28182、CVE-2024-27316、CVE-2024-31309、CVE-2024-30255、CVE-2024-24549。
- 250 MB ファイル送信のタイムアウトを修正しました。
- 直近の送信データが空でサンプルをクリックしたときの例外を修正しました。
- レポート生成の例外を修正しました。
- リソースの競合による vm_reported_error の発生を減らすために、システムパラメータを調整しました。
- スタンドアロンからクラスタへの移行を修正しました。

バージョン 2.19.2

このリリースでは、UCS M6 ハードウェアアプライアンスがデータ破棄を正常に実行できない問題が解決されています。

バージョン 2.19.1

このリリースでは、旧世代のハードウェアで今後バージョンをアップグレードする際に影響する容量不足が解消されています。また、UCS M6 の誤ったサービス通知が削除されています。

アップグレードすると移行が実行されるため、アプライアンスの起動に通常よりも時間がかかります。アプライアンスで移行が完了するまで 30 分かかります。

バージョン 2.19.0

このリリースでは、コア アプリケーション ソフトウェアが更新され、その他のさまざまな修正と機能拡張が含まれています。

- コア アプリケーション ソフトウェアが更新され、クラウドバージョン 3.5.129 に一致するようになりました。
- 起動中および設定プロセス中に誤ったエラーメッセージが表示される可能性がある軽微な問題を修正しました。
- サポートスナップショットのダウンロードに 1 分以上かかると失敗する問題を修正しました。
- クリーン インターフェイスとダーティ インターフェイスを介した ping が tgsh で許可されるようになりました。
- Kibana（管理ポータルのダッシュボードで使用）が Grafana に置き換えられました。
- セキュリティ修正、バグ修正

既知の問題

- ファームウェアの更新は、更新プロセス中に適用できない場合があります。これが発生した場合、これらの更新は再設定が正常に実行された後のリブートプロセス時に再試行されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。