Cisco Secure Workload リリースノート、リリース 3.7.1.51

初版：2023 年 6 月 22 日

最終更新：2023 年 6 月 30 日

はじめに

このドキュメントでは、Cisco Secure Workload ソフトウェアパッチリリース 3.7.1.51 の機能、バグ修正、および動作の変更について説明します。このパッチは、Cisco Secure Workload ソフトウェアのメジャーリリース 3.7.1.5 に関連付けられています。メジャーリリースの詳細については、こちらを参照してください。

ベストプラクティスとして、メジャー バージョン アップグレードを実行する前に、クラスタにパッチを適用して使用可能な最新のパッチバージョンにすることを推奨します。詳細については、『Cisco Secure Workload アップグレードガイド』（英語）を参照してください。

リリースバージョンと日付

バージョン：3.7.1.51

日付：2023 年 6 月 22 日

新機能および変更された機能に関する情報

この項では、このリリースの新機能と拡張機能、および既知の動作を示します。

互換性に関する情報

互換性の詳細については、Cisco.com の「プラットフォーム情報」を参照してください。

既知の動作

Cisco Secure Workload メジャーリリース 3.7.1.5 のリリースノートを参照してください。

拡張機能

- ソフトウェアエージェントで、VLAN タグ付きフレームによって伝送されるフローが処理されます。

- NetFlowおよびASAコネクタの報告されたフローでクライアントを検出する機能が強化されました。
- ソフトウェアエージェントを使用して SUSE Linux Enterprise Server（SLES）ワークロードのフォレンジックイベントをキャプチャする機能が強化されました。
- [フロー検索（Flow Search）] ページの TCP フラグで、AIX ワークロードの拒否されたフローが表示されます。
- [ワークロードプロファイル（Workload Profile）] ページに 2022 の CVE が表示されるようになりました。

検証済みスケーラビリティの制限値

次の表に、Cisco Secure Workload（39-RU）、Cisco Secure Workload M（8-RU）、および Cisco Secure Workload Virtual の拡張性の制限を示します。

表 *1 : Cisco Secure Workload*（*39-RU*）の拡張性の制限

設定可能なオプション	規模
ワークロードの数	最大 25000（VM またはベアメタル） すべてのセンサーが会話モードの場合、最大 50,000（2x）。
1 秒あたりのフロー機能	最大 200 万。
ハードウェア エージェント対応 Cisco Nexus 9000 シリーズ スイッチの数	最大 100（非推奨）。

表 *2 : Cisco Secure Workload M*（*8-RU*）の拡張性の制限

設定可能なオプション	規模
ワークロードの数	最大 5,000（VM またはベアメタル） すべてのセンサーが会話モードの場合、最大 10,000（2x）。
1 秒あたりのフロー機能	最大 500,000。
ハードウェア エージェント対応 Cisco Nexus 9000 シリーズ スイッチの数	最大 100（非推奨）。

表 *3 : Cisco Secure Workload Virtual*（*VMWare ESXi*）の拡張性の制限

設定可能なオプション	規模
ワークロードの数	最大 1,000（VM またはベアメタル）

設定可能なオプション	規模
1 秒あたりのフロー機能	最大 70,000。
ハードウェア エージェント対応 Cisco Nexus 9000 シリーズ スイッチの数	サポート対象外。

（注） サポートされているスケールは、最初に制限に達したパラメータに基づいています。

解決済みおよび未解決の問題

このリリースで解決済みの問題と未解決の問題には、Cisco Bug Search Tool を使用してアクセスできます。この Web ベースのツールから、この製品やその他のシスコハードウェアおよびソフトウェア製品での問題と脆弱性に関する情報を保守するシスコ バグ トラッキング システムにアクセスできます。

Cisco Bug Search Tool の詳細については、Bug Search Tool（BST）ヘルプおよび FAQ を参照してください。

（注） Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントがない場合は、アカウントを登録できます。

解決済みの問題

ID	見出し
CSCwe21841	両方のポートが既知の場合、クライアントサーバーを決定するために度合いモデルを有効にする必要がある。
CSCwf78123	[Linux] iptables-legacy が存在する場合、新しいプラットフォームでポリシーの逸脱/修正が継続的に発生する。
CSCwe83822	3.7.1.22 からの Windows エージェントのアップグレードが MSI 署名チェックに失敗する場合がある。
CSCwf18991	AIX：Catch-all が DENY の場合、DHCP が機能しない。
CSCwf29111	ポリシー分析で、Windows ワークロードによって拒否されたフローが誤って表示される場合がある。
CSCwf29138	Windows ワークロードで TetSen.exe プロセスに障害が発生する。
CSCwf37266	AIX 適用ルールが、先頭にゼロが含まれるサブネットでは正しく一致しない。

ID	見出し
CSCwf68114	NetScaler：外部オーケストレータの注釈に cluster_name がない。
CSCwf78551	WSS がクラッシュし、非常にビジーなクラスタでエージェントの再接続が頻繁に発生することがある。

未解決の問題

ID	見出し
CSCwb80213	vNIC がベアメタルサーバーでハングアップし、回復するにはサーバーの再起動が必要
CSCwf78123	[Linux] iptables-legacy が存在する場合、新しいプラットフォームでポリシーの逸脱/修正が継続的に発生する。
CSCwb91717	保留状態のソフトウェアエージェントの SW ステータスのアップグレードチャートのデータがない
CSCwb42177	ライブポリシーと適用ポリシーの分析：テーブルにカーソルを合わせると、範囲列とテキストが切り取られる
CSCwb39541	タイムアウトしている Investigate Traffic クエリのエラーメッセージを変更
CSCwc63711	Azure セグメンテーションのアクセス許可がない
CSCwd67224	AIX 7.x で適用が有効になると、フラグメンテーションが原因でエージェントが CSW クラスタに接続できない
CSCwd60340	リリース 3.6 からダウンロードしたエージェントインストーラスクリプトでリリース 3.7 のセンサーがダウンロードされない
CSCwd93604	フローの取り込み率が非常に高いクラスタで druid のロードキューが高くなる

（注） 識別子をクリックして、シスコのバグ検索ツールにアクセスし、その問題に関する詳細情報を表示します。

関連資料

ドキュメント	説明
Cisco Secure Workload Cluster Deployment Guide	Cisco Secure Workload（39-RU） プラットフォームと Cisco Secure Workload M（8-RU）のシングルおよびデュアルラックインストールの物理的な構成、設置場所の準備、およびケーブル配線について説明します。 Cisco Tetration（Cisco Secure Workload）M5 クラスタハードウェア導入ガイド
Cisco Secure Workload Virtual Deployment Guide	Cisco Secure Workload 仮想アプライアンス（旧称 Tetration-V）の展開について説明します。 Cisco Secure Workload Virtual (Tetration-V) Deployment Guide
Cisco Secure Workload プラットフォームのデータシート	Cisco Secure Workload プラットフォームのデータシート
Cisco Secure Workload のドキュメント	Cisco Secure Workload のドキュメント
最新の脅威データソース	Cisco Secure Workload

シスコへのお問い合わせ

上記のオンライン リソースでは問題を解決できない場合は、Cisco TAC にお問い合わせください。

- Cisco TAC の電子メール アドレス：tac@cisco.com
- Cisco TAC の電話番号（北米）：1.408.526.7209 または 1.800.553.2447
- Cisco TAC の連絡先（世界全域）：Cisco Worldwide Support の連絡先

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。