シスコ脆弱性データベース（VDB）アップデート 342 リリースノート

Cisco Vulnerability Database について

シスコ脆弱性データベース（VDB）は、オペレーティング システム、クライアント、およびアプリケーションのフィンガープリントだけでなく、ホストが影響を受ける可能性がある既知の脆弱性のデータベースです。システムでは、VDB を使用して、特定のホストで感染のリスクが高まるかどうかを判断します。

シスコでは、VDB に対して定期的に更新を提供しています。Firepower Management Center で VDB と関連付けられたマッピングの更新にかかる時間は、ネットワーク マップ内のホストの数によって異なります。一般的に、更新の実行にかかるおおよその時間（分）を判断するには、ホストの数を 1000 で割ります。

VDB の更新は、Cisco.com の VDB ソフトウェアのダウンロードページで確認することができます。

Cisco Firepower Application Detector リファレンスについて

『Cisco Firepower Application Detector リファレンス』には、リリースノートと、VDB リリースでサポートされているアプリケーションディテクタに関する情報が含まれています。本リファレンスに記載されている各アプリケーションについては、次の情報を確認できます。

- 説明：アプリケーションの簡単な説明。
- カテゴリ：アプリケーションの最も重要な機能を説明する一般分類。カテゴリの例としては、「Web サービスプロバイダ」、「e-コマース」、「広告ポータル」、および「ソーシャルネットワーキング」などがあります。
- タグ：アプリケーションに関する追加情報を表示する事前定義のタグ。タグの例としては、「Web メール」、「SSL プロトコル」、「ファイルの共有/転送」、および「広告の表示」などがあります。アプリケーションには、0 個、1 個、または複数個のタグが割り当てられています。
- リスク：アプリケーションが組織のセキュリティポリシーに違反しうる目的で使用される可能性。リスクのレベルは次のとおりです。「非常に高い」、「高」、「中」、「低」、および「非常に低い」。
- ビジネスとの関連性：アプリケーションが、娯楽目的ではなく組織の事業運営の範囲で使用される可能性。関連性のレベルは次のとおりです。「非常に高い」、「高」、「中」、「低」、および「非常に低い」。

サポートされるプラットフォームとソフトウェア バージョン

このガイドは、次のプラットフォームのソフトウェア バージョンでインストールされる脆弱性データベース アップデートに関するガイドです。

Sourcefire 3D システム/Firepower システム バージョン 5.x：

- Cisco FireSIGHT Management Centers（旧 Defense Centers）

Firepower バージョン 6.x：

- Cisco Firepower Management Centers（旧 Defense Centers/FireSIGHT Management Centers）

サポートされるディテクタ タイプ

サポートされているディテクタ タイプは次のとおりです。

- アプリケーション プロトコル
- クライアント
- Web アプリケーション

脆弱性データベースアップデート 342 でサポートされるアプリケーションの合計数

シスコ脆弱性データベース（VDB）アップデート 342 は、3,628 種類のアプリケーションをサポートしています。

脆弱性データベースアップデート 342 変更ログ

ここでは、VDB 341（2021 年 1 月 29 日 8:02:48 PM UTC）から VDB 342（2021 年 3 月 29 日 8:56:05 PM UTC）までの変更を示します。

アプリケーション プロトコル ディテクタ

合計追加数：	59
合計削除数：	0
合計更新数	5

クライアント ディテクタ

合計追加数：	0
合計削除数：	0
合計更新数	1

Web アプリケーション ディテクタ

合計追加数：	2
合計削除数：	17
合計更新数	19

FireSIGHT/Firepower ディテクタの更新

合計追加数：	0
合計削除数：	0
合計更新数	0

オペレーティング システム フィンガープリントの詳細

合計追加数：	0
合計削除数：	0
合計更新数	0

オペレーティング システムおよびハードウェア フィンガープリントの詳細

合計追加数：	0
合計削除数：	0

合計更新数	0

脆弱性の参照

合計追加数：	107
合計削除数：	0
合計更新数	0

フィンガープリントの参照

合計追加数：	0
合計削除数：	0
合計更新数	0

ファイル タイプ ディテクタ

合計追加数：	0
合計削除数：	0
合計更新数	0

オペレーティング システム フィンガープリントの詳細：

- 追加または変更なし

オペレーティング システムおよびハードウェア フィンガープリントの詳細：

- 追加または変更なし

フィンガープリント参照の詳細：

- 追加または変更なし

アプリケーション プロトコル ディテクタ：

- GRPC：Google が開発したリモートプロシージャコール。（追加）
- NDMP：カバレッジを追加するために変更（更新）
- RTSP：カバレッジを追加するために変更（更新）
- RADIUS：カバレッジを追加するために変更（更新）
- QUIC：UDP フローのカバレッジを追加するために変更（更新）
- IEC 104 初期化の終了：アプリケーションの説明を更新（更新）
- IEC 104 TESTFR CON：テストフレーム確認の IEC 104 機能。（追加）

- IEC 104 TESTFR ACT：テスト フレーム アクティベーションの IEC 104 機能。（追加）
- IEC 104 STARTDT CON：データ転送開始確認の IEC 104 機能。（追加）
- IEC 104 STARTDT ACT：データ転送開始アクティベーションの IEC 104 機能。（追加）
- IEC 104 ダブルポイント情報：IEC 104 タイプ ID、M_DP_NA_1。ダブルポイント情報のモニタ方向のプロセス情報。（追加）
- IEC 104 モニタビットストリング 32 ビット：IEC 104 タイプ ID、M_BO_NA_1。ビットストリング 32 ビットのモニタ方向のプロセス情報。（追加）
- IEC 104 正規化の測定：IEC 104 タイプ ID、M_ME_NA_1。測定値のモニタ方向、正規化された値のプロセス情報。（追加）
- IEC 104 拡張の測定：IEC 104 タイプ ID、M_ME_NB_1。測定値のモニタ方向、拡張された値のプロセス情報。（追加）
- IEC 104 統合合計：IEC 104 タイプ ID、M_IT_NA_1。統合された合計のモニタ方向のプロセス情報。（追加）
- IEC 104 パック単一ポイント：IEC 104 タイプ ID、M_PS_NA_1。ステータス変更検出を含むパックされた単一ポイント情報のモニタ方向のプロセス情報。（追加）
- IEC 104 品質記述子のない正規化の測定：IEC 104 タイプ ID、M_ME_ND_1。測定値のモニタ方向、品質記述子のない正規化された値のプロセス情報。（追加）
- IEC 104 長時間のダブルポイント情報：IEC 104 タイプ ID、M_DP_TB_1。時間タグ CP56Time2a を持つダブルポイント情報のプロセステレグラム。（追加）
- IEC 104 長時間のステップ位置情報：IEC 104 タイプ ID、M_ST_TB_1。時間タグ CP56Time2a を持つステップ位置情報のプロセステレグラム。（追加）
- IEC 104 長時間のビットストリング 32 ビット：IEC 104 タイプ ID、M_BO_TB_1。時間タグ CP56Time2a を持つビットストリング 32 ビットのプロセステレグラム。（追加）
- IEC 104 長時間の拡張の測定：IEC 104 タイプ ID、M_ME_TE_1。測定値、時間タグ CP56Time2a を持つ拡張された値のプロセステレグラム。（追加）
- IEC 104 長時間の単精度浮動の測定：IEC 104 タイプ ID、M_ME_TF_1。測定値、時間タグ CP56Time2a を持つ短い浮動小数点値のプロセステレグラム。（追加）
- IEC 104 長時間の統合合計：IEC 104 タイプ ID、M_IT_TB_1。時間タグ CP56Time2a を持つ統合された合計のプロセステレグラム。（追加）
- IEC 104 長時間の保護のイベント：IEC 104 タイプ ID、M_EP_TD_1。時間タグ CP56Time2a を持つ保護装置のイベントのプロセステレグラム。（追加）
- IEC 104 長時間のパック開始イベント：IEC 104 タイプ ID、M_EP_TE_1。時間タグ CP56Time2a を持つ保護装置のパックされた開始イベントのプロセステレグラム。（追加）
- IEC 104 長時間のパック出力回路情報：IEC 104 タイプ ID、M_EP_TF_1。時間タグ CP56Time2a を含む保護装置のパックされた出力回路情報のプロセステレグラム。（追加）

- IEC 104 長時間の単一コマンド：IEC 104 タイプ ID、C_SC_TA_1。時間タグ CP56Time2a を持つ単一コマンドのコマンドテレグラム。（追加）
- IEC 104 長時間のダブルコマンド：IEC 104 タイプ ID、C_DC_TA_1。時間タグ CP56Time2a を持つダブルコマンドのコマンドテレグラム。（追加）
- IEC 104 長時間の規制ステップコマンド：IEC 104 タイプ ID、C_RC_TA_1。時間タグ CP56Time2a を持つ規制ステップコマンドのコマンドテレグラム。（追加）
- IEC 104 長時間のセットポイントコマンド正規化：IEC 104 タイプ ID、C_SE_TA_1。セットポイントコマンド、時間タグ CP56Time2a を持つ正規化された値のコマンドテレグラム。（追加）
- IEC 104 長時間のセットポイントコマンド拡張：IEC 104 タイプ ID、C_SE_TB_1。セットポイントコマンド、時間タグ CP56Time2a を持つ拡張された値のコマンドテレグラム。（追加）
- IEC 104 長時間のセットポイントコマンド単精度浮動：IEC 104 タイプ ID、C_SE_TC_1。セットポイントコマンド、時間タグ CP56Time2a を持つ単精度浮動小数点値のコマンドテレグラム。（追加）
- IEC 104 長時間のビットストリング 32 ビットコマンド：IEC 104 タイプ ID、C_BO_TA_1。時間タグ CP56Time2a を持つビットストリング 32 ビットのコマンドテレグラム。（追加）
- IEC 104 カウンタ問い合わせコマンド：IEC 104 タイプ ID、C_CI_NA_1。カウンタ問い合わせコマンドの制御方向のシステム情報。（追加）
- IEC 104 読み取りコマンド：IEC 104 タイプ ID、C_RD_NA_1。読み取りコマンドの制御方向のシステム情報。（追加）
- IEC 104 クロック同期コマンド：IEC 104 タイプ ID、C_CS_NA_1。クロック同期コマンドの制御方向のシステム情報。（追加）
- IEC 104 リセットプロセスコマンド：IEC 104 タイプ ID、C_RP_NC_1。リセットプロセスコマンドの制御方向のシステム情報。（追加）
- IEC 104 長時間のテストコマンド：IEC 104 タイプ ID、C_TS_TA_1。時間タグ CP56Time2a を持つテストコマンドの制御方向のシステム情報。（追加）
- IEC 104 正規化の測定のパラメータ：IEC 104 タイプ ID、P_ME_NA_1。測定値の制御方向、正規化された値のパラメータ。（追加）
- IEC 104 拡張の測定のパラメータ：IEC 104 タイプ ID、P_ME_NB_1。測定値の制御方向、拡張された値のパラメータ。（追加）
- IEC 104 単精度浮動の測定のパラメータ：IEC 104 タイプ ID、P_ME_NC_1。測定値の制御方向、単精度浮動小数点値のパラメータ。（追加）
- IEC 104 パラメータ アクティベーション：IEC 104 タイプ ID、P_AC_NA_1。パラメータアクティベーションの制御方向のパラメータ。（追加）

- IEC 104 ファイル準備完了：IEC 104 タイプ ID、F_FR_NA_1。ファイル転送のファイル準備完了。（追加）
- IEC 104 セクション準備完了：IEC 104 タイプ ID、F_SR_NA_1。ファイル転送のセクション準備完了。（追加）
- IEC 104 ディレクトリの呼び出し、ファイルの選択：IEC 104 タイプ ID、F_SC_NA_1。ディレクトリの呼び出し、ファイルの選択、ファイルの呼び出し、セクションの呼び出し。（追加）
- IEC 104 最後のセクション最後のセグメント：IEC 104 タイプ ID、F_LS_NA_1。ファイル転送の最後のセクション、最後のセグメント。（追加）
- IEC 104 Ack ファイル Ack セクション：IEC 104 タイプ ID、F_AF_NA_1。ファイル転送の Act ファイル、Act セクション。（追加）
- IEC 104 リストセグメント：IEC 104 タイプ ID、F_SG_NA_1。ファイル転送のリストセグメント。（追加）
- IEC 104 リストディレクトリ：IEC 104 タイプ ID、F_DR_TA_1。ファイル転送のリストディレクトリ。（追加）
- IEC 104 クエリログ：IEC 104 タイプ ID、F_SC_NB_1。ファイル転送のクエリログ。（追加）
- Modbus Read Coils：Read Coils コマンドは、Modbus シリアル通信プロトコルの機能コードです。（追加）
- Modbus Read Discrete Inputs：Read Discrete Inputs コマンドは、Modbus シリアル通信プロトコルの機能コードです。（追加）
- Modbus Read Hold Registers：Read Holding Registers コマンドは、Modbus シリアル通信プロトコルの機能コードです。（追加）
- Modbus Read Input Registers：Read Input Registers コマンドは、Modbus シリアル通信プロトコルの機能コードです。（追加）
- Modbus Write Single Coil：Write Single Coil コマンドは、Modbus シリアル通信プロトコルの機能コードです。（追加）
- Modbus Write Single Register：Write Single Register コマンドは、Modbus シリアル通信プロトコルの機能コードです。（追加）
- Modbus Write Multiple Coils：Write Multiple Coils コマンドは、Modbus シリアル通信プロトコルの機能コードです。（追加）
- Modbus Write Multiple Registers：Write Multiple Registers コマンドは、Modbus シリアル通信プロトコルの機能コードです。（追加）
- Modbus Read File Record：Read File Record コマンドは、Modbus シリアル通信プロトコルの機能コードです。（追加）

- Modbus Write File Record：Write File Record コマンドは、Modbus シリアル通信プロトコルの機能コードです。（追加）
- Modbus Mask Write Register：Mask Write Register コマンドは、Modbus シリアル通信プロトコルの機能コードです。（追加）
- Modbus Read/Write Multiple Registers：Read/Write Multiple Registers コマンドは、Modbus シリアル通信プロトコルの機能コードです。（追加）
- Modbus Read FIFO Queue：Read FIFO Queue コマンドは、Modbus シリアル通信プロトコルの機能コードです。（追加）
- Modbus Encapsulated Interface Transport：Modbus Encapsulated Interface Transport コマンドは、Modbus シリアル通信プロトコルの機能コードです。（追加）

クライアント ディテクタ：

- TextMe：Web クライアントをカバーするパターンを追加（更新）

Web アプリケーション ディテクタ：

- Hopster：クーポンサイト（削除）
- J&R：コンピュータおよび電子機器の小売業者（削除）
- Writeboard：コラボレーションのための Web ベーステキストエディタ（削除）
- Diamond Dash：Facebook 向けのマッチングゲーム（削除）
- Family Tree：Facebook の家族向けソーシャル ネットワーキング アプリ（削除）
- Google Maps：「復号化されたトラフィック」タグを追加（更新）
- Babylon：「検索エンジン」カテゴリから削除（更新）
- Yellow Pages：「ビデオの共有」および「マルチメディア（TV /ビデオ）」のタグを削除（更新）
- Yandex：「Web メール」タグを削除（更新）
- Redbox Instant：レンタルおよびオンラインの映画/ゲーム（削除）
- Microsoft Excel：カバレッジを追加するために変更（更新）
- Boxoh：さまざまな配送プロバイダーからの荷物のトラッキングを集約するサイト（削除）
- Adenin：「検索エンジン」カテゴリから削除（更新）
- Squidoo：ソーシャルブログサイト（削除）
- Wikispaces：Wiki のホスティングサイト（削除）
- 24/7 Media：広告サイト（削除）
- Effective Measure：アプリケーションの名前を「Narratiive」に変更（更新）

- Nugg：広告サイト（削除）
- Yabuka：広告サイト（削除）
- X Plus One：広告サイト（削除）
- DC Storm：広告サイト（削除）
- Ultrasurf：Firefox ブラウザからのトラフィックの誤検出を修正するように変更（更新）
- PointRoll：広告会社（削除）
- ESPN Video：カバレッジを追加するために変更（更新）
- Amazon Cloud Drive：カバレッジを追加するために変更（更新）
- Amazon Cloud Drive のアップロード：カバレッジを追加するために変更（更新）
- Myspace Music：カバレッジを追加するために変更（更新）
- Mgoon：韓国のエンターテイメント Web ポータル（削除）
- Seterus：融資処理の会社（削除）
- Cassandra：無料のオープンソース NoSQL データベース管理システム（追加）
- Yum：RPM ベースの Linux オペレーティングシステム用のパッケージ管理ツール（追加）
- TeamViewer：カバレッジを追加するために変更（更新）
- Facebook：カバレッジを追加するために変更（更新）
- Google：カバレッジを追加するために変更（更新）
- Microsoft：カバレッジを追加するために変更（更新）
- Microsoft Azure：カバレッジを追加するために変更（更新）
- VPN Monster：UDP カバレッジを追加するために変更（更新）
- Orange：復号パターンのカバレッジを追加（更新済み）

FireSIGHT/Firepower ディテクタの更新：

- 追加または変更なし

ファイル タイプ ディテクタの詳細：

- 追加または変更なし

Snort ID の脆弱性の参照の詳細：

- CVE 2013-2028 - Snort 参照 ID 108、16、8（追加）
- CVE 2014-3120 - Snort 参照 ID 33830、36256、44690、57129、57130、57131（追加）
- CVE 2015-0050 - Snort 参照 ID 33053、33358（追加）

- CVE 2017-0199 - Snort 参照 ID 42189、42190、42229、42230、42231、45519、45520、52481、52482、57063、57064、57065、57066（追加）
- CVE 2017-8965 - Snort 参照 ID 57188（追加）
- CVE 2017-11882 - Snort 参照 ID 44989、44990、45132、45133、45134、45135、45466、45467、45511、45512、49775、49776、50684、50685、53090、54620、54621、57054、57055（追加）
- CVE 2017-18344 - Snort 参照 ID 57156、57157（追加）
- CVE 2018-1156 - Snort 参照 ID 57176、57177（追加）
- CVE 2018-11472 - Snort 参照 ID 57126、57127（追加）
- CVE 2018-11473 - Snort 参照 ID 57178、57179（追加）
- CVE 2019-5544 - Snort 参照 ID 57111、57112（追加）
- CVE 2019-11707 - Snort 参照 ID 50518、50519、57180、57181（追加）
- CVE 2019-19781 - Snort 参照 ID 300001、52512、52513、52603、52620、52662（追加）
- CVE 2020-4006 - Snort 参照 ID 57182、57183、57184、57185（追加）
- CVE 2020-6088 - Snort 参照 ID 53126（追加）
- CVE 2020-13546 - Snort 参照 ID 55991、55992（追加）
- CVE 2020-13548 - Snort 参照 ID 56063、56064（追加）
- CVE 2020-13550 - Snort 参照 ID 56048、56049、56050（追加）
- CVE 2020-13561 - Snort 参照 ID 56158、56159、56160、56161（追加）
- CVE 2020-13562 - Snort 参照 ID 56145、56146（追加）
- CVE 2020-13563 - Snort 参照 ID 56143、56144（追加）
- CVE 2020-13564 - Snort 参照 ID 56145、56146（追加）
- CVE 2020-13565 - Snort 参照 ID 56152、56153（追加）
- CVE 2020-13572 - Snort 参照 ID 56365、56366（追加）
- CVE 2020-13574 - Snort 参照 ID 56211、56275（追加）
- CVE 2020-13575 - Snort 参照 ID 56507、56508（追加）
- CVE 2020-13576 - Snort 参照 ID 56509、56510（追加）
- CVE 2020-13577 - Snort 参照 ID 56307、56308（追加）
- CVE 2020-13578 - Snort 参照 ID 56297、56298（追加）
- CVE 2020-13579 - Snort 参照 ID 56226、56227、56228、56229（追加）

- CVE 2020-13580 - Snort 参照 ID 56212、56213（追加）
- CVE 2020-13581 - Snort 参照 ID 56209、56210（追加）
- CVE 2020-13582 - Snort 参照 ID 56199（追加）
- CVE 2020-13585 - Snort 参照 ID 56451、56452（追加）
- CVE 2020-13586 - Snort 参照 ID 56389、56390（追加）
- CVE 2020-13942 - Snort 参照 ID 56990（追加）
- CVE 2020-13951 - Snort 参照 ID 56989（追加）
- CVE 2020-14343 - Snort 参照 ID 56223、56224（追加）
- CVE 2020-16846 - Snort 参照 ID 57048、57049（追加）
- CVE 2020-25159 - Snort 参照 ID 57155（追加）
- CVE 2020-27247 - Snort 参照 ID 56526、56527（追加）
- CVE 2020-27248 - Snort 参照 ID 56526、56527（追加）
- CVE 2020-27249 - Snort 参照 ID 56526、56527（追加）
- CVE 2020-27250 - Snort 参照 ID 56526、56527（追加）
- CVE 2020-28595 - Snort 参照 ID 56727、56728（追加）
- CVE 2021-1138 - Snort 参照 ID 56955（追加）
- CVE 2021-1139 - Snort 参照 ID 56953（追加）
- CVE 2021-1140 - Snort 参照 ID 56938、56939、56940、56941（追加）
- CVE 2021-1141 - Snort 参照 ID 56945（追加）
- CVE 2021-1142 - Snort 参照 ID 56955（追加）
- CVE 2021-1247 - Snort 参照 ID 56947（追加）
- CVE 2021-1248 - Snort 参照 ID 56954（追加）
- CVE 2021-1264 - Snort 参照 ID 56950（追加）
- CVE 2021-1272 - Snort 参照 ID 56956（追加）
- CVE 2021-1280 - Snort 参照 ID 56893、56894（追加）
- CVE 2021-1289 - Snort 参照 ID 57087、57093（追加）
- CVE 2021-1290 - Snort 参照 ID 57091（追加）
- CVE 2021-1291 - Snort 参照 ID 57094（追加）
- CVE 2021-1292 - Snort 参照 ID 57088、57089（追加）

- CVE 2021-1293 - Snort 参照 ID 57097（追加）
- CVE 2021-1294 - Snort 参照 ID 57076（追加）
- CVE 2021-1295 - Snort 参照 ID 57092（追加）
- CVE 2021-1296 - Snort 参照 ID 57074（追加）
- CVE 2021-1297 - Snort 参照 ID 57072（追加）
- CVE 2021-1298 - Snort 参照 ID 56946（追加）
- CVE 2021-1299 - Snort 参照 ID 56942、56943、56944（追加）
- CVE 2021-1302 - Snort 参照 ID 56957（追加）
- CVE 2021-1304 - Snort 参照 ID 56958、56959、56960、56961、56962（追加）
- CVE 2021-1305 - Snort 参照 ID 56963（追加）
- CVE 2021-1314 - Snort 参照 ID 57086（追加）
- CVE 2021-1315 - Snort 参照 ID 57086（追加）
- CVE 2021-1316 - Snort 参照 ID 57086（追加）
- CVE 2021-1317 - Snort 参照 ID 57095、57096（追加）
- CVE 2021-1318 - Snort 参照 ID 57084、57085（追加）
- CVE 2021-1319 - Snort 参照 ID 57090（追加）
- CVE 2021-1320 - Snort 参照 ID 57069（追加）
- CVE 2021-1321 - Snort 参照 ID 57069（追加）
- CVE 2021-1322 - Snort 参照 ID 57101（追加）
- CVE 2021-1323 - Snort 参照 ID 57068（追加）
- CVE 2021-1324 - Snort 参照 ID 57068（追加）
- CVE 2021-1325 - Snort 参照 ID 57090（追加）
- CVE 2021-1327 - Snort 参照 ID 57082（追加）
- CVE 2021-1328 - Snort 参照 ID 57077（追加）
- CVE 2021-1329 - Snort 参照 ID 57113（追加）
- CVE 2021-1330 - Snort 参照 ID 57114（追加）
- CVE 2021-1331 - Snort 参照 ID 57099（追加）
- CVE 2021-1332 - Snort 参照 ID 57098（追加）
- CVE 2021-1333 - Snort 参照 ID 57073（追加）

- CVE 2021-1334 - Snort 参照 ID 57073（追加）
- CVE 2021-1335 - Snort 参照 ID 57113（追加）
- CVE 2021-1336 - Snort 参照 ID 57110（追加）
- CVE 2021-1337 - Snort 参照 ID 57109（追加）
- CVE 2021-1338 - Snort 参照 ID 57075（追加）
- CVE 2021-1339 - Snort 参照 ID 57102（追加）
- CVE 2021-1340 - Snort 参照 ID 57102（追加）
- CVE 2021-1341 - Snort 参照 ID 57105（追加）
- CVE 2021-1342 - Snort 参照 ID 57077（追加）
- CVE 2021-1343 - Snort 参照 ID 57078、57079、57080、57081（追加）
- CVE 2021-1344 - Snort 参照 ID 57113（追加）
- CVE 2021-1345 - Snort 参照 ID 57114（追加）
- CVE 2021-1346 - Snort 参照 ID 57083（追加）
- CVE 2021-1347 - Snort 参照 ID 57100（追加）
- CVE 2021-1348 - Snort 参照 ID 57113（追加）
- CVE 2021-1648 - Snort 参照 ID 57061、57062（追加）
- CVE 2021-2109 - Snort 参照 ID 57158、57159（追加）
- CVE 2021-21017 - Snort 参照 ID 57137、57138（追加）
- CVE 2021-25274 - Snort 参照 ID 57161（追加）

支援が必要な場合

Cisco Firepower デバイスに関するマニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス リクエストの送信、追加情報の収集の詳細については、『What's New in Cisco Product Documentation』を参照してください。

『What's New in Cisco Product Documentation』は、シスコの新規および改訂版の技術マニュアルの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。Cisco ASA デバイスに関してご質問がある場合や支援が必要な場合は、以下のシスコ サポートに連絡してください。

- 注：TAC リクエストを開くには、Cisco.com ユーザ ID を最初に登録する必要があります。
- Cisco.com ユーザ ID を作成したら、サービス要求のステータス オンラインを開始またはチェックするか、電話で TAC に問い合わせることができます。
  - 米国：1-800-553-2447 無料通話
  - 国際サポート番号
- TAC からテクニカル サポートを受ける方法の詳細については、『Technical Support Reference Guide』（PDF、1 MB）を参照してください。

Talos について

Talos Security Intelligence and Research Group（Talos）は、洗練されたシステムによってサポートされる優れた脅威研究者によって構成され、既知の脅威と新たな脅威の両方を検出および分析し、その脅威から保護するためのシスコ製品の脅威インテリジェンスを作成しています。Talos は、Snort.org、ClamAV、SenderBase.org、および SpamCop の公式ルール セットも保守しています。このチームの専門知識には、ソフトウェア開発、リバースエンジニアリング、脆弱性トリアージ、マルウェア調査、および情報収集が含まれています。