シスコ脆弱性データベース（VDB）アップデート 333 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 Reference』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 333 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 333 では、3,643 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 333 の変更ログ

この項では、VDB 332（UTC 2020 年 2 月 18 日午後 5 時 18 分 02 秒）から DVB 333（UTC 2020 年 3 月 30 日午後 9 時 09 分 31 秒）への変更について説明します。

アプリケーション プロトコル ディテクタ

合計追加数：	3
合計削除数：	1
合計更新数	4

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	2

Web アプリケーション ディテクタ

合計追加数：	12
合計削除数：	0
合計更新数	3

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	19

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：	0
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：

- ISO SAP：サービスアクセスポイント（SAP）は、ISO ネットワーキングのエンドシステムです（削除）。
- ISO MMS：検出性能が向上しました（更新）。
- IEC 60870-5-104：コマンドに基づく高精度な検出を提供するため、検出機能が改善されました（更新）。
- IEC 104 単一：IEC 104 コマンド（追加）。
- MMS getNameList：MMS コマンド（追加）。

- DNS over TLS：TLS を介して DNS クエリと応答を暗号化および送信するためのセキュリティプロトコル（追加）。
- DNS：トラフィックフローを適切に分類するために更新されました（更新）。
- TLS：メモリ使用量を改善するために更新されました（更新）。

クライアント ディテクタ：

- Telegram：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Kik Messenger：トラフィックフローを適切に分類するために更新されました。（更新済み）

Web アプリケーション ディテクタ：

- Windscribe：誤検出を回避するために変更されました（更新）。
- Microsoft Teams：Microsoft Teams は、職場での情報交換を目的としたユニファイドコミュニケーションおよびコラボレーション プラットフォームです。
- GoToMeeting：検出機能を強化するために変更されました（更新）。
- Citrix Online：検出機能を強化するために変更されました（更新）。
- AMP：AMP は Web コンポーネント フレームワークであり、Web サイトのパブリッシングテクノロジーです（追加）。
- Tidal：Tidal は、サブスクリプションベースの音楽、ポッドキャスト、およびビデオ ストリーミング サービスです（追加）。
- Appier：Appier は、人工知能（AI）プラットフォームの提供を目的とするテクノロジー企業です（追加）。
- Tappx：Tappx は、収益化と相互プロモーションを目的としたオープンなアプリ開発者コミュニティです（追加）。
- NrData：カテゴリ B の ISP（追加）
- Twinkl：Twinkl 教育リソースの公式 Web サイト（追加）
- ZeroDHA：オンライン株式仲買業に焦点を当てた金融サービス会社（追加）
- Ballina Beach Village：休暇を過ごすリゾートを予約し、旅行を計画するための Web サイト（追加）
- TAFE NSW：TAFE NSW はオーストラリアの教育およびトレーニングコース向けの主要プロバイダーです（追加）。
- DepartAppWeb：データの測定、収集、分析、およびレポート作成を目的としたプラットフォーム（追加）
- Stripe：Stripe は支払い処理プラットフォームを提供します（追加）。

FireSIGHT/Firepower ディテクタの更新：

- Citrix GoToMeeting Platform：誤検出を修正するために更新されました（更新）。
- Imo.im: トラフィックフローを適切に分類するために更新されました。（更新済み）
- Drift：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Zscaler：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Cloudinary：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Princess Polly：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Coolmath：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Stile：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Noteflight：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Onshape：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Prodigy Games：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Adobe Fonts：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Firefly Education：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Walkme：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Honey：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Grammarly：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Font Awesome：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Catholic Education Australia：トラフィックフローを適切に分類するために更新されました。（更新済み）
- Workplace by Facebook：トラフィックフローを適切に分類するために更新されました。（更新済み）

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：

- 追加または変更なし

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。