シスコ脆弱性データベース（VDB）アップデート 337 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 337 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 337 では、3,665 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 337 の変更ログ

このセクションでは、VDB 336（2020 年 6 月 15日 16:39:44 UTC）から VDB 337（2020 年 7 月 10 日 16:52:14 UTC）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：	0
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	2

Web アプリケーション ディテクタ

合計追加数：	15
合計削除数：	0
合計更新数	10

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	7

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：

このリリースでは、National Vulnerability Database（NVD）による最新の脆弱性データを同期するため、より合理化された方法を導入しました。この変更により、最新の脆弱性の参照を、現在の IPS ルールおよび公開された NVD データと直接同期できます。

- 最終更新日：2020 年 7 月 2 日
- 脆弱性の総数：11,146
- 83,000 個のソフトウェアエントリを更新し、古いソフトウェアエントリを廃止しました。

ソフトウェアエントリの最適化は、VDB パッケージ全体のサイズを 10 MB の範囲にまで削減するのにも役立ちました。

アプリケーション プロトコル ディテクタ：

- Battle.net：誤検出を回避するためにディテクタを変更（更新済み）

- SSL：新しいメタデータを抽出するためにディテクタを変更（更新済み）
- DNS：新しいメタデータを抽出するためにディテクタを変更（更新済み）
- IMAP：検出を改善するためにディテクタを変更（更新済み）
- HTTP：トンネル化されたフローを区別するためにディテクタを変更（更新済み）

クライアント ディテクタ：

- Psiphon：プロキシ経由のフローの検出を改善するためにディテクタを変更（更新済み）
- Ultrasurf：プロキシ経由のフローの検出を改善するためにディテクタを変更（更新済み）

Web アプリケーション ディテクタ：

- Bing Maps：カバレッジを改善するためにディテクタを変更（更新済み）
- MTv：カバレッジを改善するためにディテクタを変更（更新済み）
- VPN Masterカバレッジを改善するためにディテクタを変更（更新済み）
- Adobe Update：Adobe ソフトウェアの更新（追加）
- DriveHQ：クラウドストレージおよびオンライン バックアップ システム（追加）
- IEC 104 制御ビットストリング 32 ビット：IoT ベースのディテクタ（追加）
- IEC 104 ダブルコマンド: IoT ベースのディテクタ（追加）
- IEC 104 問い合わせコマンド：IoT ベースのディテクタ（追加）
- IEC 104 規制ステップコマンド：IoT ベースのディテクタ（追加）
- IEC 104 Setpoint コマンド正規化：IoT ベースのディテクタ（追加）
- IEC 104 Setpoint コマンド拡張：IoT ベースのディテクタ（追加）
- IEC 104 Setpoint コマンド単精度浮遊：IoT ベースのディテクタ（追加）
- IEC 104 初期化の終了：IoT ベースのディテクタ（追加）
- IEC 104 長時間の正規化の測定：IoT ベースのディテクタ（追加）
- IEC 104 長時間の単一ポイント情報：IoT ベースのディテクタ（追加）
- IEC 104 ステップ位置情報：IoT ベースのディテクタ（追加）
- IEC 104 単精度浮動の測定：IoT ベースのディテクタ（追加）
- IEC 104 単一ポイント情報：IoT ベースのディテクタ（追加）
- Twitter：カバレッジを改善するためにディテクタを変更（更新済み）
- Box：カバレッジを改善するためにディテクタを変更（更新済み）
- Blizzard：カバレッジを改善するためにディテクタを変更（更新済み）

- Wii：カバレッジを改善するためにディテクタを変更（更新済み）
- DuckDuckGo：Safesearchのカバレッジを改善するためにディテクタを変更（更新済み）
- eRoom：ニンテンドーゲームトラフィックの誤検出を削除するためにディテクタを変更（更新済み）
- Zoom：特定の UDP トラフィックのカバレッジを追加するためにディテクタを変更（更新済み）

FireSIGHT/Firepower ディテクタの更新：

- QQ：検出とメモリ使用量を改善するためにディテクタを変更（更新済み）
- OpenVPN：検出とメモリ使用量を改善するためにディテクタを変更（更新済み）
- RTP：検出とメモリ使用量を改善するためにディテクタを変更（更新済み）
- Fuze：RTP トラフィックでの誤検出を回避するためにディテクタを変更（更新済み）
- Exchangeカバレッジを改善するためにディテクタを変更（更新済み）
- Salesforce.comカバレッジを改善するためにディテクタを変更（更新済み）
- Microsoft：カバレッジを改善するためにディテクタを変更（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。