シスコ脆弱性データベース（VDB）アップデート 340 リリース ノート

シスコ脆弱性データベースについて

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 340 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 340 では、3,571 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 340 変更ログ

このセクションでは、VDB 339（UTC 2020 年 11 月 5 日午後 9 時 41 分 10 秒）から VDB 340（UTC 2020 年 12 月 16 日午前 12 時 15 分 58 秒）までの変更点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	0

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：	23
合計更新数	15

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：	54
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：

- QUIC：Quic バージョン 50 のカバレッジを追加（更新）
- SNMP：SNMP フローを検出するためのカバレッジを追加（更新）
- SSL：SSL として分類される一部の HTTP2 フローの誤検出を修正（更新）
- DNS：フローを適切に検出するためにディテクタを更新（更新）
- UDP：さらにメタデータを抽出するためにディテクタを更新（更新）

クライアント ディテクタ：

- 追加または変更なし

Web アプリケーション ディテクタ：

- Plaxo：連絡先情報の自動更新を提供する、オンラインアドレス帳およびソーシャル ネットワーキング サービス。（削除）。
- AOL Instant Messenger：AOL のインターネット チャット クライアント。（削除）。
- AOL Instant Messenger Netscape：AOL Instant Messenger - Netscape。（削除）。
- Scottrade：ディスカウント ブローカレッジ サービス。（削除）。
- Vehix：新車および中古車の情報および販売の Web サイト。（削除）。
- GOGOBOX：中国に拠点を置く Web ポータル。（削除）。
- Suresome：Web ベースの暗号化されたプロキシサービス。（削除）。
- Steam：カバレッジのパターンを追加（更新）
- Pool Live：Facebook のビリヤードゲーム。（削除）。
- Datei.to：ドイツのファイル共有サービス。（削除）。
- Apple Mobile Yahoo API：Apple 製品用の Yahoo のモバイルアプリケーション。（削除）。
- Magicland：Facebook のゲームアプリケーション。（削除）。
- Jdistatic：クラウドベースのバックアップサービス。（削除）。
- BackWeb：自動バックグラウンド ソフトウェア ダウンロードおよびインストールを可能にするソフトウェア。（削除）。
- JetSetMe：ユーザの世界中の動きを追跡できるモバイルアプリケーション。（削除）。
- Chinaren：中国のソーシャル ネットワーキング サイト。（削除）。
- UltraViolet：クラウドベースの動画ストリーミングサービス。（削除）。
- Instagram Images：Instagram の画像を表示する際に生成されるトラフィック、Instagram を推奨して廃止。（削除）。
- Instagram Video：Instagram のビデオを表示する際に生成されるトラフィック、Instagram を推奨して廃止。（削除）。
- Songsari：オンラインおよびメディア ファイル ダウンロードのための韓国の Web ポータル。（削除）。
- Yandex Music：カバレッジのパターンを追加（更新）
- Yandex Video：カバレッジのパターンを追加（更新）
- Best Arabic Games：アラビア語のオンラインカジノ。（削除）。
- PandaTv：ゲーマー向けのライブ ストリーミング ビデオ プラットフォーム。（削除）。
- YNews：全般的な ybreakingnews.com Web サイトのトラフィック。（削除）。

- Adult World：アダルトビデオ。（削除）。
- Instagram Media：Instagram の画像とビデオを表示する際に生成されるトラフィック。（追加）
- TikTok：以前の Musical.ly カバレッジをカバーする新しいディテクタを追加。（追加）
- Staples：カバレッジを追加（更新）
- Google Translate：Web サイトの地理的パターンを追加（更新）
- GoDaddy：カバレッジのパターンを追加（更新）
- BlueStacks：カバレッジのパターンを追加（更新）
- Angry Birds：カバレッジのパターンを追加（更新）
- Turbo VPN：カバレッジのパターンを追加（更新）
- Zynga Poker：カバレッジのパターンを追加（更新）
- DotVPN：カバレッジのパターンを追加（更新）
- Gom VPN：カバレッジのパターンを追加（更新）
- Express VPN：カバレッジのパターンを追加（更新）
- Sony：Webサイトの地理的パターンを追加（更新）
- Facebook Video：カバレッジを追加（更新）

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：2017-11284 - Snort 参照 ID 56407、56406、46937（追加）
- CVE：2018-18264 - Snort 参照 ID 56439 （追加）
- CVE：2019-11580 - Snort 参照 ID 56436（追加）
- CVE：2019-12630 - Snort 参照 ID 56407、56406、46937（追加）
- CVE：2019-1621 - Snort 参照 ID 50514、56306（追加）
- CVE：2019-18257 - Snort 参照 ID 56386、56385、56384、56383（追加）
- CVE：2019-2904 - Snort 参照 ID 56499、56498、56497（追加）
- CVE：2019-7192 - Snort 参照 ID 56521、56520 （追加）

- CVE：2020-10243 - Snort 参照 ID 56525、56524、56523（追加）
- CVE：2020-14625 - Snort 参照 ID 56445、37859（追加）
- CVE：2020-1472 - Snort 参照 ID 56290、55802、55704、55703（追加）
- CVE：2020-14882 - Snort 参照 ID 56203、56202、56201、56200（追加）
- CVE：2020-15299 - Snort 参照 ID 56325、56324（追加）
- CVE：2020-15999 - Snort 参照 ID 56133、56132、56131、56130（追加）
- CVE：2020-16998 - Snort 参照 ID 56255、56254（追加）
- CVE：2020-17010 - Snort 参照 ID 56264、56263（追加）
- CVE：2020-17038 - Snort 参照 ID 56262、56261（追加）
- CVE：2020-17047 - Snort 参照 ID 56309（追加）
- CVE：2020-17051 - Snort 参照 ID 56312、56311（追加）
- CVE：2020-17052 - Snort 参照 ID 56287、56286（追加）
- CVE：2020-17053 - Snort 参照 ID 56289、56288（追加）
- CVE：2020-17056 - Snort 参照 ID 56302、56301（追加）
- CVE：2020-17057 - Snort 参照 ID 56260、56259（追加）
- CVE：2020-17061 - Snort 参照 ID 56305、56304、56303（追加）
- CVE：2020-17087 - Snort 参照 ID 56231、56230（追加）
- CVE：2020-17088 - Snort 参照 ID 56296、56295（追加）
- CVE：2020-1747 - Snort 参照 ID 56224、56223（追加）
- CVE：2020-24948 - Snort 参照 ID 56519（追加）
- CVE：2020-26072 - Snort 参照 ID 56448（追加）
- CVE：2020-26567 - Snort 参照 ID 56364（追加）
- CVE：2020-27125 - Snort 参照 ID 56408（追加）
- CVE：2020-27130 - Snort 参照 ID 56423、56422、56421、56420、56419、56418、56417、56416、56415、56414、56405、56404（追加）
- CVE：2020-27131 - Snort 参照 ID 56413、56412、56411、56410、56409、56408、56407、56406、46937（追加）
- CVE：2020-3367 -Snort 参照 ID 49992、49993、49994、49995（追加）
- CVE：2020-3371 - Snort 参照 ID 47698（追加）
- CVE：2020-3392 - Snort 参照 ID 56447（追加）

- CVE：2020-3470 - Snort 参照 ID 56440、56441、56442、56443、56444（追加）
- CVE：2020-3531 - Snort 参照 ID 56431（追加）
- CVE：2020-3556 - Snort 参照 ID 56221、56222（追加）
- CVE：2020-3573 - Snort 参照 ID 56216、56217（追加）
- CVE：2020-3586 - Snort 参照 ID 56424（追加）
- CVE：2020-3588 - Snort 参照 ID 56225（追加）
- CVE：2020-3603 - Snort 参照 ID 56216、56217（追加）
- CVE：2020-3604 - Snort 参照 ID 56218、56219（追加）
- CVE：2020-4206 - Snort参照ID 56430、56429、56428、56427（追加）
- CVE：2020-4208 - Snort 参照 ID 56321（追加）
- CVE：2020-4241 - Snort 参照 ID 56435、56434、56433、56432（追加）
- CVE：2020-6147 - Snort 参照 ID 54308、54309（追加）
- CVE：2020-6148 - Snort 参照 ID 54310、54311（追加）
- CVE：2020-6149 - Snort 参照 ID 54312、54313（追加）
- CVE：2020-6150 - Snort 参照 ID 54314、54315（追加）
- CVE：2020-6155 - Snort 参照 ID 54415、54416（追加）
- CVE：2020-6156 - Snort 参照 ID 54430、54431（追加）
- CVE： 2020-6549 - Snort 参照 ID 56438、56437（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。