シスコ脆弱性データベース（VDB）アップデート 327 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。

Cisco Talos Intelligence Group（Talos） では、VDB の定期的な更新を配布しています。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 Reference』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 プロバイダー」、「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 327 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 327 は、3,619 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 327 変更ログ

このセクションでは、VDB 325（2019 年 7 月 12 日、UTC 午後 1 時 26 分 52 秒）から VDB 327（2019 年 8 月 27 日、UTC 午後 2 時 22 分 42 秒）への変更について説明しています。

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	0

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：	0
合計削除数：	0
合計更新数	0

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：	1

合計更新数	5

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：	1
合計更新数	4

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	1

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：

- Google または Ubuntu または CentOS または Red Hat Android、CrOS または Linux または Enterprise Linux Android 2.3、4.0、4.1、4.2、4.3、4.4、CrOS 3701.81.2 または Linux 11.04、12.10、13.04 または Linux 6.3、6.4、または Enterprise Linux 7.0（ID 30959）（削除）
- Ubuntu または CentOS または Red Hat Linux または Enterprise Linux 13.10、14.04、16.04、16.10 または CentOS 7.2、7.3 または Enterprise Linux 7.5、7.6（ID 952）（更新）
- Microsoft Windows Vista、7、Server 2008、8、10、Server 2012、Server 2012 R2、Server 2016、Windows Phone 7.5、8.0（ID 30932）（更新）
- Google または Ubuntu または CentOS または Red Hat Android または CrOS または Linux または Enterprise Linux Android 2.2、2.3、3.2、4.0、4.1、4.2、4.3、4.4、5.0、5.1、7.0 または Linux 11.04、12.10、13.04、13.10、14.04、16.04、16.10 または CentOS 6.3、6.4、7.2、7.3 または Enterprise Linux 7.0、7.5、7.6 または CrOS 3701.81.2（ID 30941）（更新）
- Apple iOS 9.0、9.1、9.2、9.3、10.0、10.2、11.0、11.1、11.2、11.3、11.4、12.0、12.1、12.2（ID 60203）（更新）
- Red Hat Enterprise Linux 7.0、7.5、7.6（ID 60207）（更新）

フィンガープリント参照の詳細：

- フィンガープリント ID 30959 リファレンス（削除）
- フィンガープリント ID 952 リファレンス（更新）
- フィンガープリント ID 30932 リファレンス（更新）
- フィンガープリント ID 30941 リファレンス（更新）
- フィンガープリント ID 60207 リファレンス（更新）

アプリケーション プロトコル ディテクタ：

- 追加または変更なし

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：

- 追加または変更なし

FireSIGHT/Firepower ディテクタの更新：

- Facebook：Facebook アプリケーション検出を改善
- QQ：QQ および NetBios の検出を改善
- XVPN：XVPN アプリケーションの検出を改善
- GoToMeeting：GoToMeeting の検出を改善
- QUIC：Quic Q046 プロトコルのサポートを追加
- Internet Download Manager：Internet Download Manager のフローの検出を改善
- HTTP：HTTP トラフィックの検出を改善

ファイル タイプ ディテクタの詳細：

- SWF フラッシュ ファイル（ID 44）（更新）

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。