シスコ脆弱性データベース（VDB）アップデート 338 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 338 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 338 では、3,659 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 338 変更ログ

このセクションでは、VDB 337（2020 年 7 月 10 日 16:52:14 UTC）から VDB 338（2020 年 9 月 24 日 13:00:29 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	3

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：	4
合計削除数：	10
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	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：	196
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：

- whois：説明が変更され、リスクが非常に高い値から低い値に変更されました（更新）
- ISCSI：カバレッジが追加されました（更新）
- HTTP/2：名前が HTTP 2.0 から RFC 標準に準拠するように変更されました。（更新済み）

クライアント ディテクタ：

- Microsoft CryptoAPI：Office 365 タグが追加されました（更新）

Web アプリケーション ディテクタ：

- Bebo：ソーシャルネットワーキングおよびブログ。（削除）。

- Octopz：Web ベースのコラボレーションツール。（削除）。
- Tetris Battle：Facebook のテトリス（削除）
- Playdom：Facebook ゲームをプロデュースする Web ゲーム会社。（削除）。
- Readability：記事をよりクリーンな形式に変換するブラウザプラグインおよびモバイルアプリ。（削除）。
- Triggit：広告を生成するマーケティングサービス。（削除）。
- Nexage：広告サイト。（削除）。
- Nimbuzz：インスタントメッセージングおよび SMS。（削除）。
- Vube：ビデオのアップロードおよび共有サイト。（削除）。
- Quant Code：全般的な quant-code.com Web サイトのトラフィック。（削除）。
- Skype：Office 365 タグが追加されました（更新）
- Skype for Business：Office 365 タグが追加されました（更新）
- Apple News：アプリに SSL タグが追加されました（更新）
- Zoom アップロード：Zoom でファイルをアップロードするアクション。（追加）
- Zoom ダウンロード：Zoom からのファイルのダウンロード。（追加）
- Zoom ミーティング：Zoom での会議への参加。（追加）
- Twilio：グローバル規模で構築された API で SMS、音声、およびメッセージング アプリケーションを構築するためのクラウド通信プラットフォーム。（追加）

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：2005-4438 - Snort 参照 ID 17282（追加）
- CVE：2005-4438 - Snort 参照 ID 54578（追加）
- CVE：2010-4326 - Snort 参照 ID 18768（追加）
- CVE：2017-12477 - Snort 参照 ID 54495（追加）
- CVE：2017-8539 - Snort 参照 ID 54788（追加）
- CVE：2017-8539 - Snort 参照 ID 54787（追加）
- CVE：2018-13329 - Snort 参照 ID 54774（追加）

- CVE：2018-13329 - Snort 参照 ID 54773（追加）
- CVE：2018-13353 - Snort 参照 ID 53970（追加）
- CVE：2018-13353 - Snort 参照 ID 53969（追加）
- CVE：2018-13353 - Snort 参照 ID 53968（追加）
- CVE：2018-13353 - Snort 参照 ID 53967（追加）
- CVE：2018-13358 - Snort 参照 ID 53970（追加）
- CVE：2018-13358 - Snort 参照 ID 53969（追加）
- CVE：2018-13358 - Snort 参照 ID 53968（追加）
- CVE：2018-13358 - Snort 参照 ID 53967（追加）
- CVE：2018-13418 - Snort 参照 ID 53970（追加）
- CVE：2018-13418 - Snort 参照 ID 53969（追加）
- CVE：2018-13418 - Snort 参照 ID 53968（追加）
- CVE：2018-13418 - Snort 参照 ID 53967（追加）
- CVE：2018-15715 - Snort 参照 ID 54616（追加）
- CVE：2018-15715 - Snort 参照 ID 54615（追加）
- CVE：2018-15715 - Snort 参照 ID 54614（追加）
- CVE：2018-15715 - Snort 参照 ID 54613（追加）
- CVE：2019-12725 - Snort 参照 ID 54797（追加）
- CVE：2019-12725 - Snort 参照 ID 54796（追加）
- CVE：2019-12725 - Snort 参照 ID 54795（追加）
- CVE：2019-12725 - Snort 参照 ID 54794（追加）
- CVE：2019-13567 - Snort 参照 ID 54637（追加）
- CVE：2019-13567 - Snort 参照 ID 54636（追加）
- CVE：2019-13567 - Snort 参照 ID 54728（追加）
- CVE：2019-13567 - Snort 参照 ID 54727（追加）
- CVE：2019-13688 - Snort 参照 ID 54498（追加）
- CVE：2019-13688 - Snort 参照 ID 54497（追加）
- CVE：2019-9081 - Snort 参照 ID 54603（追加）
- CVE：2019-9081 - Snort 参照 ID 54602（追加）

- CVE：2019-9082 - Snort 参照 ID 54903（追加）
- CVE：2020-0605 - Snort 参照 ID 54619（追加）
- CVE：2020-0605 - Snort 参照 ID 54618（追加）
- CVE：2020-10713 - Snort 参照 ID 54757（追加）
- CVE：2020-10713 - Snort 参照 ID 54756（追加）
- CVE：2020-1147 - Snort 参照 ID 54511（追加）
- CVE：2020-1147 - Snort 参照 ID 54629（追加）
- CVE：2020-1147 - Snort 参照 ID 54684（追加）
- CVE：2020-1147 - Snort 参照 ID 54790（追加）
- CVE：2020-1147 - Snort 参照 ID 54789（追加）
- CVE：2020-11901 - Snort 参照 ID 54706（追加）
- CVE：2020-11901 - Snort 参照 ID 54705（追加）
- CVE：2020-12027 - Snort 参照 ID 54671（追加）
- CVE：2020-12027 - Snort 参照 ID 54670（追加）
- CVE：2020-12028 - Snort 参照 ID 54674（追加）
- CVE：2020-12028 - Snort 参照 ID 54672（追加）
- CVE：2020-12029 - Snort 参照 ID 54675（追加）
- CVE：2020-12029 - Snort 参照 ID 54673（追加）
- CVE：2020-1300 - Snort 参照 ID 54527（追加）
- CVE：2020-1300 - Snort 参照 ID 54526（追加）
- CVE：2020-1337 - Snort 参照 ID 54820（追加）
- CVE：2020-1337 - Snort 参照 ID 54819（追加）
- CVE：2020-1337 - Snort 参照 ID 54818（追加）
- CVE：2020-1337 - Snort 参照 ID 54817（追加）
- CVE：2020-1350 - Snort 参照 ID 54518（追加）
- CVE：2020-1350 - Snort 参照 ID 54577（追加）
- CVE：2020-1350 - Snort 参照 ID 54576（追加）
- CVE：2020-1350 - Snort 参照 ID 54575（追加）
- CVE：2020-13522 - Snort 参照 ID 54581（追加）

- CVE：2020-13522 - Snort 参照 ID 54582（追加）
- CVE：2020-13523 - Snort 参照 ID 54579（追加）
- CVE：2020-13523 - Snort 参照 ID 54580（追加）
- CVE：2020-1362 - Snort 参照 ID 54593（追加）
- CVE：2020-1362 - Snort 参照 ID 54592（追加）
- CVE：2020-1362 - Snort 参照 ID 54591（追加）
- CVE：2020-1362 - Snort 参照 ID 54590（追加）
- CVE：2020-13693 - Snort 参照 ID 54597（追加）
- CVE：2020-13693 - Snort 参照 ID 54596（追加）
- CVE：2020-1374 - Snort 参照 ID 54523（追加）
- CVE：2020-1380 - Snort 参照 ID 54744（追加）
- CVE：2020-1380 - Snort 参照 ID 54743（追加）
- CVE：2020-1381- Snort 参照 ID 54522（追加）
- CVE：2020-1381- Snort 参照 ID 54521（追加）
- CVE：2020-1382 - Snort 参照 ID 54515（追加）
- CVE：2020-1382 - Snort 参照 ID 54514（追加）
- CVE：2020-1382 - Snort 参照 ID 54513（追加）
- CVE：2020-1382 - Snort 参照 ID 54512（追加）
- CVE：2020-1399 - Snort 参照 ID 54535（追加）
- CVE：2020-1399 - Snort 参照 ID 54534（追加）
- CVE：2020-1403 - Snort 参照 ID 54510（追加）
- CVE：2020-1403 - Snort 参照 ID 54509（追加）
- CVE：2020-1410 - Snort 参照 ID 54533（追加）
- CVE：2020-1410 - Snort 参照 ID 54532（追加）
- CVE：2020-1410 - Snort 参照 ID 54531（追加）
- CVE：2020-1410 - Snort 参照 ID 54530（追加）
- CVE：2020-1410 - Snort 参照 ID 54529（追加）
- CVE：2020-1410 - Snort 参照 ID 54528（追加）
- CVE：2020-1426 - Snort 参照 ID 54517（追加）

- CVE：2020-1426 - Snort 参照 ID 54516（追加）
- CVE：2020-14645 - Snort 参照 ID 54755（追加）
- CVE：2020-1480 - Snort 参照 ID 54746（追加）
- CVE：2020-1480 - Snort 参照 ID 54745（追加）
- CVE：2020-14946 - Snort 参照 ID 54556（追加）
- CVE：2020-1529 - Snort 参照 ID 54738（追加）
- CVE：2020-1529 - Snort 参照 ID 54737（追加）
- CVE：2020-1566 - Snort 参照 ID 54766（追加）
- CVE：2020-1566 - Snort 参照 ID 54765（追加）
- CVE：2020-1567 - Snort 参照 ID 54742（追加）
- CVE：2020-1567 - Snort 参照 ID 54741（追加）
- CVE：2020-1570 - Snort 参照 ID 54740（追加）
- CVE：2020-1570 - Snort 参照 ID 54739（追加）
- CVE：2020-1578 - Snort 参照 ID 54754（追加）
- CVE：2020-1578 - Snort 参照 ID 54753（追加）
- CVE：2020-1584 - Snort 参照 ID 54736（追加）
- CVE：2020-1584 - Snort 参照 ID 54735（追加）
- CVE：2020-1587 - Snort 参照 ID 54734（追加）
- CVE：2020-1587 - Snort 参照 ID 54733（追加）
- CVE：2020-1956 - Snort 参照 ID 54650（追加）
- CVE：2020-1956 - Snort 参照 ID 54649（追加）
- CVE：2020-3140 - Snort 参照 ID 54568（追加）
- CVE：2020-3144 - Snort 参照 ID 54557（追加）
- CVE：2020-3145 - Snort 参照 ID 54564（追加）
- CVE：2020-3145 - Snort 参照 ID 54560（追加）
- CVE：2020-3145 - Snort 参照 ID 54561（追加）
- CVE：2020-3145 - Snort 参照 ID 54562（追加）
- CVE：2020-3145 - Snort 参照 ID 54563（追加）
- CVE：2020-3146 - Snort 参照 ID 54564（追加）

- CVE：2020-3146 - Snort 参照 ID 54560（追加）
- CVE：2020-3146 - Snort 参照 ID 54561（追加）
- CVE：2020-3146 - Snort 参照 ID 54562（追加）
- CVE：2020-3146 - Snort 参照 ID 54563（追加）
- CVE：2020-3323 - Snort 参照 ID 54548（追加）
- CVE：2020-3323 - Snort 参照 ID 54549（追加）
- CVE：2020-3323 - Snort 参照 ID 54550（追加）
- CVE：2020-3323 - Snort 参照 ID 54551（追加）
- CVE：2020-3330 - Snort 参照 ID 54544（追加）
- CVE：2020-3331 - Snort 参照 ID 54548（追加）
- CVE：2020-3331 - Snort 参照 ID 54549（追加）
- CVE：2020-3331 - Snort 参照 ID 54550（追加）
- CVE：2020-3331 - Snort 参照 ID 54551（追加）
- CVE：2020-3332 - Snort 参照 ID 54538（追加）
- CVE：2020-3332 - Snort 参照 ID 54539（追加）
- CVE：2020-3332 - Snort 参照 ID 54540（追加）
- CVE：2020-3332 - Snort 参照 ID 54541（追加）
- CVE：2020-3338 - Snort 参照 ID 54899（追加）
- CVE：2020-3357 - Snort 参照 ID 54542（追加）
- CVE：2020-3357 - Snort 参照 ID 54543（追加）
- CVE：2020-3358 - Snort 参照 ID 54552（追加）
- CVE：2020-3376 - Snort 参照 ID 54656（追加）
- CVE：2020-3381 - Snort 参照 ID 54553（追加）
- CVE：2020-3383 - Snort 参照 ID 54668（追加）
- CVE：2020-3383 - Snort 参照 ID 53504（追加）
- CVE：2020-3383 - Snort 参照 ID 54667（追加）
- CVE：2020-3384 - Snort 参照 ID 54655（追加）
- CVE：2020-3386 - Snort 参照 ID 54696（追加）
- CVE：2020-3386 - Snort 参照 ID 54697（追加）

- CVE：2020-3386 - Snort 参照 ID 54698（追加）
- CVE：2020-3386 - Snort 参照 ID 54699（追加）
- CVE：2020-3386 - Snort 参照 ID 54700（追加）
- CVE：2020-3387 - Snort 参照 ID 54545（追加）
- CVE：2020-3387 - Snort 参照 ID 54546（追加）
- CVE：2020-3387 - Snort 参照 ID 54547（追加）
- CVE：2020-3398 - Snort 参照 ID 54896（追加）
- CVE：2020-3433 - Snort 参照 ID 54694（追加）
- CVE：2020-3433 - Snort 参照 ID 54695（追加）
- CVE：2020-3452 - Snort 参照 ID 54598（追加）
- CVE：2020-3452 - Snort 参照 ID 54599（追加）
- CVE：2020-3452 - Snort 参照 ID 54600（追加）
- CVE：2020-3452 - Snort 参照 ID 54601（追加）
- CVE：2020-3928 - Snort 参照 ID 54617（追加）
- CVE：2020-5902 - Snort 参照 ID 54462（追加）
- CVE：2020-5902 - Snort 参照 ID 54484（追加）
- CVE：2020-5903 - Snort 参照 ID 54462（追加）
- CVE：2020-6070 - Snort 参照 ID 53004（追加）
- CVE：2020-6070 - Snort 参照 ID 53005（追加）
- CVE：2020-6098 - Snort 参照 ID 53562（追加）
- CVE：2020-6100 - Snort 参照 ID 53545（追加）
- CVE：2020-6100 - Snort 参照 ID 53546（追加）
- CVE：2020-6101 - Snort 参照 ID 52842（追加）
- CVE：2020-6101 - Snort 参照 ID 52843（追加）
- CVE：2020-6102 - Snort 参照 ID 53553（追加）
- CVE：2020-6102 - Snort 参照 ID 53554（追加）
- CVE：2020-6103 - Snort 参照 ID 53549（追加）
- CVE：2020-6103 - Snort 参照 ID 53550（追加）
- CVE：2020-6114 - Snort 参照 ID 53944（追加）

- CVE：2020-6114 - Snort 参照 ID 53945（追加）
- CVE：2020-6145 - Snort 参照 ID 54290（追加）
- CVE：2020-6286 - Snort 参照 ID 54572（追加）
- CVE：2020-6286 - Snort 参照 ID 54571（追加）
- CVE：2020-6287 - Snort 参照 ID 54574（追加）
- CVE：2020-6287 - Snort 参照 ID 54573（追加）
- CVE：2020-6287 - Snort 参照 ID 54572（追加）
- CVE：2020-6287 - Snort 参照 ID 54571（追加）
- CVE：2020-6390 - Snort 参照 ID 54623（追加）
- CVE：2020-6390 - Snort 参照 ID 54622（追加）
- CVE：2020-6651 - Snort 参照 ID 54583（追加）
- CVE：2020-7980 - Snort 参照 ID 54824（追加）
- CVE：2020-8617 - Snort 参照 ID 54630（追加）
- CVE：2020-9802 - Snort 参照 ID 54666（追加）
- CVE：2020-9802 - Snort 参照 ID 54665（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。