



ネットワーク セキュリティ アドバイザリの の識別

- [セキュリティアドバイザリの概要](#) (1 ページ)
- [セキュリティアドバイザリの表示](#) (1 ページ)

セキュリティアドバイザリの概要

Cisco Product Security Incident Response Team (PSIRT; プロダクトセキュリティ インシデント レスポンスチーム) は、シスコ製品のセキュリティインシデントに対応し、セキュリティ脆弱性ポリシーを規制し、[シスコのセキュリティアドバイザリとアラート](#)を推奨します。

セキュリティアドバイザリ ツールは、これらの推奨されるアドバイザリを使用して、Cisco DNA Center内のインベントリをスキャンし、既知の脆弱性を持つデバイスを検出します。

セキュリティアドバイザリの表示

始める前に

- セキュリティアドバイザリ ツールを使用するには、[機械推論パッケージ](#)をインストールする必要があります。Cisco *Digital Network Architecture Center* 管理者ガイド [英語] の「[Download and Install Packages and Updates](#)」を参照してください。
- オブザーバとして Cisco DNA Center にログインすると、ホームページで [Security Advisories] ツールを表示できません。

ステップ 1 Cisco DNA Center のホームページで、[Tools] エリアまで下にスクロールし、[Security Advisories] をクリックします。右上隅の  アイコンをクリックし、[Security Advisories] を選択することもできます。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan] をクリックします。

Cisco DNA Center Cisco DNA Center は、セキュリティの問題を特定して自動分析を改善するために、ナレッジベースを使用します。最新のセキュリティアドバイザリを表示するには、定期的にナレッジベースを更新することをお勧めします。

- a)  > [System Settings] > [Settings] > [Machine Reasoning] をクリックします。
- b) [Import Latest from Cisco] をクリックするか、[ここ](#)をクリックして最新の使用可能なナレッジベースをダウンロードし、[Import from local] をクリックします。
- c) 自動更新に登録するには、[AUTO UPDATE] トグルボタンをクリックします。

- (注)
- セキュリティアドバイザリ ダッシュボードにはシスコが公開しているセキュリティアドバイザリが表示されます。アドバイザリは現行のソフトウェアイメージに基づいており、ネットワーク上のデバイスに影響する場合があります。脆弱性が実際に存在するかどうかを判断するには、設定、プラットフォームの詳細、またはその他の基準をさらに詳しく分析する必要があります。
 - セキュリティアドバイザリ スキャンのサポートは、サポートされている最小ソフトウェアバージョンに準拠しているルータおよびスイッチでのみ使用できます。サポートされている最小のソフトウェアバージョンの詳細については、「[Cisco DNA Centerサポート対象デバイス](#)」を参照してください。
 - 表示されるセキュリティアドバイザリは、[シスコのセキュリティ脆弱性ポリシー](#)に基づいています。

次の表に、使用できる情報を記載します。

| カラム | 説明 |
|--------------|--------------------------------------------------------------------------------------------|
| アドバイザリ ID | ネットワークで検出されたセキュリティアドバイザリの ID。 |
| アドバイザリタイトル | ネットワークデバイスに適用されるセキュリティ脆弱性アドバイザリの名前。アドバイザリをクリックして、それぞれのアドバイザリ Web ページに移動します。 |
| CVSS スコア | 共通脆弱性評価システム (CVSS) モデルに基づいて評価されたスコア。 |
| Impact | ネットワークへの脆弱性の影響 (Critical、High、Medium、Low など)。 |
| CVE | 脆弱性の Common Vulnerabilities and Exposures (CVE) 識別子。 |
| デバイス | 脆弱性の影響を受けるデバイスの数。この特定のアドバイザリに基づいて脆弱性が存在する可能性のあるデバイスを表示するには、番号をクリックし、必要に応じてデバイスをアップグレードします。 |
| 検出以降の期間 (日数) | 脆弱性が検出されてからの経過日数。 |
| Last Updated | アドバイザリが最後に更新された日付。 |

ステップ 3 各デバイスに適用可能なアドバイザリの数を表示するには、[Devices] タブをクリックします。

- a) デバイスに一致するものをすべて表示するには、アドバイザリの数をクリックします。

- b) デバイストポロジを表示するには、右上隅にあるトポロジアイコンをクリックします。トポロジ内のデバイスをクリックすると、そのデバイスに一致するすべてのアドバイザリが表示されます。
- デバイスの横にあるロックアイコンは、デバイスに適用可能な1つ以上のアドバイザリがあることを示します。

ステップ4 いつでも [Scan] をクリックすれば、表示された結果を更新できます。
