

# Cisco IoT Field Network Directorの脆弱性



アドバイザーID : [cisco-sa-iot-fnd-dos-n8N26Q4u](#) [CVE-2026-20169](#)  
初公開日 : 2026-05-06 16:00 [CVE-2026-20167](#)  
バージョン 1.0 : Final [CVE-2026-20168](#)  
CVSSスコア : [7.7](#)  
回避策 : No workarounds available  
Cisco バグ ID : [CSCwm80968](#)  
[CSCwm81015](#) [CSCwm81008](#)

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

## 概要

Cisco IoT Field Network Director(IOND)ソフトウェアのWebベースの管理インターフェイスにおける複数の脆弱性により、認証されたりリモートの攻撃者が、管理対象ルータ上でファイルへのアクセス、コマンドの実行、およびサービス妨害(DoS)状態を引き起こす可能性があります。

これらの脆弱性の詳細については本アドバイザーの「詳細情報」セクションを参照してください。

シスコはこれらの脆弱性に対処するソフトウェアアップデートをリリースしています。これらの脆弱性に対処する回避策はありません。

このアドバイザーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iot-fnd-dos-n8N26Q4u>

## 該当製品

### 脆弱性のある製品

これらの脆弱性は、デバイスの設定に関係なく、Cisco IoT Field Network Directorに影響を与えます。

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザーの「修正済みソフトウェア」セクションを参照してください。

脆弱性を含んでいないことが確認された製品

このアドバイザリの「[脆弱性のある製品](#)」セクションに記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。

## 詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

### CVE-2026-20167: Cisco IoT Field Network DirectorのリモートデバイスのDoS脆弱性

Cisco IoT Field Network Director(IFND)のWebベース管理インターフェ이스の脆弱性により、権限の低い認証されたリモートの攻撃者が、リモート管理されているルータにDoS状態を引き起こす可能性があります。

この脆弱性は、不適切なエラー処理に起因します。攻撃者は、巧妙に細工された入力をWebベースの管理インターフェ이스に送信することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はリモートルータに不正なファイルを要求し、ルータのリロードを引き起こし、その結果DoS状態が発生する可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。この脆弱性に対処する回避策はありません。

バグID: [CSCwm81015](#)

CVE ID : CVE-2026-20167

セキュリティ影響評価 ( SIR ) : 高

CVSS ベーススコア : 7.7

CVSS ベクトル : CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

### CVE-2026-20168: Cisco IoT Field Network Directorのパストラバーサルの脆弱性

Cisco IoT Field Network Director(IFND)のWebベース管理インターフェ이스の脆弱性により、権限の低い認証されたリモートの攻撃者が、アクセス許可を持たないファイルを取得できる可能性があります。

この脆弱性は、不十分なファイルアクセスチェックに起因します。攻撃者は、Webベースの管理インターフェ이스で巧妙に細工された入力を送信することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は、アクセスが許可されていないファイルを読み取る可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。この脆弱性に

対処する回避策はありません。

バグID: [CSCwm81008](#)

CVE ID : CVE-2026-20168

セキュリティ影響評価 ( SIR ) : 中

CVSS ベーススコア : 6.5

CVSSベクトル : CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

## CVE-2026-20169: Cisco IoT Field Network Directorのコマンドインジェクションの脆弱性

Cisco IoT Field Network Director(IFND)のWebベース管理インターフェ이스の脆弱性により、権限の低い認証されたリモートの攻撃者がリモートルータでファイルにアクセスし、コマンドを実行できる可能性があります。

この脆弱性は、ユーザが指定したデータの入力検証が不十分であることに起因します。攻撃者は、Webベースの管理インターフェ이스で巧妙に細工された入力を送信することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は、リモートルータ上でユーザEXECモードでファイルを作成、読み取り、または削除し、限定されたコマンドを実行できる可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。この脆弱性に対処する回避策はありません。

バグID: [CSCwm80968](#)

CVE ID : CVE-2026-20169

セキュリティ影響評価 ( SIR ) : 中

CVSS ベーススコア : 6.4

CVSSベクトル : CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

## 回避策

これらの脆弱性に対処する回避策はありません。

## 修正済みソフトウェア

シスコでは、回避策や緩和策 ( 該当する場合 ) は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。これらの脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

## 修正済みリリース

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこれらの脆弱性に対する修正を含む最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

Cisco IoT Field Network Directorリリース	First Fixed Release ( 修正された最初のリリース )
4以前 <sup>1</sup>	修正済みリリースに移行。
5	5.0.0-117

1. Cisco IoT FNDソフトウェアリリース4.12以前は、[ソフトウェアメンテナンスが終了](#)しています。これらの脆弱性が修正済みのサポート対象リリースに移行することをお勧めします。

シスコの 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、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを検証します。

## 不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例とその公表は確認しておりません。

## 出典

シスコは、これらの脆弱性を報告していただいたBen Sina氏に感謝いたします。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iot-fnd-dos-n8N26Q4u>

## 改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2026年5月6日

## 利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な

情報が欠落していたりする可能性があります。このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。