# Cisco Nexus Dashboard OrchestratorのSSL/TLS証明書の検証における脆弱性

Medium

アドバイザリーID : cisco-sa-ndo-tlsvld-FdUF3cpw
初公開日 : 2024-10-02 16:00
バージョン 1.0 : Final
CVSSスコア : 5.9
回避策 : No workarounds available
Cisco バグ ID : CSCwi72006

CVE-2024-20385

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 Nexus Dashboard Orchestrator(NDO)のSSL/TLS実装における脆弱性により、認証されていないリモートの攻撃者が該当デバイスから機密情報を傍受する可能性があります。

この脆弱性は、Cisco NDOのピア証明書の検証サイト管理機能が、新しいサイトが追加されたとき、または既存のサイトが再登録されたときに限り、Cisco Application Policy Infrastructure Controller(APIC)、Cisco Cloud Network Controller(CNC)、およびCisco Nexusダッシュボードの証明書を検証するために存在します。攻撃者は、Machine-in-the-Middleテクニックを使用して該当デバイスとCisco NDOの間のトラフィックを代行受信し、巧妙に細工された証明書を使用して該当デバイスを偽装することにより、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、これらのデバイス間の通信中に機密情報を学習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。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndo-tlsvld-FdUF3cpw

## 該当製品

### 脆弱性のある製品

公開時点で、この脆弱性はCisco NDOに影響を与えました。

注：Cisco Nexusダッシュボードリリース3.1(1k)から、Cisco NDOはCisco Nexusダッシュボード統合リリースで配布されます。

公開時点で脆弱性が確認されている Cisco ソフトウェアのリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。最新情報については、本アドバイザリの冒頭に記載されているバグIDの「詳細」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、この脆弱性の影響を受けることが分かっています。

シスコは、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- Nexus Dashboard Fabric Controller（NDFC）
- Nexus Dashboard Insights

## 回避策

こ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

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性とアップグレード ソリューション一式を確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

### 修正済みリリース

発行時点では、次の表に示すリリース情報は正確でした。最新情報については、本アドバイザリの冒頭に記載されているバグIDの「詳細」セクションを参照してください。

左側の列にはシスコソフトウェアリリース、右側の列に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、およびこの脆弱性に対する修正を含むリリースが示されています。

| Cisco NDOリリース | First Fixed Release（修正された最初のリリース） |
|---|---|
| 4.1 以前 | 修正済みリリースに移行。 |
| 4.2 | 4.2(3o) |

| Cisco NDOリリース | First Fixed Release（修正された最初のリリース） |
|---|---|
| 4.3 以前 | 修正済みリリースに移行。 |
| 4.4 | 4.4（1.1009） |

注：Cisco Nexusダッシュボードリリース3.1(1k)から、Cisco NDOはCisco Nexusダッシュボード統合リリースで配布されます。Cisco Nexusダッシュボードリリース3.2(1e)には、Cisco NDOリリース4.4(1.1009)が含まれています。

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された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やその公表は確認しておりません。

## 出典

シスコは、この脆弱性を報告していただいたNetcloud AGのLukas Mergenthaler氏に感謝いたします。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndo-tlsvld-FdUF3cpw

## 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 | 2024年10月2日 |

## 利用規約

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。