

Cisco Prime Infrastructureの情報開示の脆弱性



アドバイザリーID : cisco-sa-pi-unauth-infodiscl-LFnLgmey

[CVE-2026-20189](#)

初公開日 : 2026-05-06 16:00

バージョン 1.0 : Final

CVSSスコア : [4.3](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwr43176](#)

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 Prime Infrastructureのログファイルダウンロード機能の脆弱性により、認証されたりリモートの攻撃者がサーバから任意のログファイルをダウンロードできる可能性があります。

この脆弱性は、ダウンロードサービスAPIでの不十分な認証チェックに起因します。攻撃者は、巧妙に細工されたURL要求を該当デバイス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、攻撃者は機密性の高いログファイルをダウンロードできるようになります。ダウンロードしなければ、アクセスの許可を得ることができません。

この脆弱性を不正利用するには、攻撃者が該当デバイスのWebベース管理インターフェイスにアクセスするための有効なクレデンシャルを持っている必要があります。

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-pi-unauth-infodiscl-LFnLgmey>

該当製品

脆弱性のある製品

公開時点では、この脆弱性はデバイス設定に関係なく、Cisco Prime Infrastructureに影響を与えていました。

このアドバイザリーの公開時点で脆弱性が存在するシスコ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。最も完全で最新の情報については、このアドバイザーの上部にあるバグ 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

このアドバイザーの[脆弱性のある製品セクション](#)にリストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性がCisco Evolved Programmable Network Manager(EPNM)には影響を与えないことを確認しました。

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

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。この脆弱性を完全に修正し、本アドバイザー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、本アドバイザー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

発行時点では、次の表に示すリリース情報は正確でした。最も完全で最新の情報については、このアドバイザーの上部にあるバグ 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ー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 Prime Infrastructure のリリース | First Fixed Release (修正された最初のリリース) |
|----------------------------------|--------------------------------------|
| 3.9 以前 | 修正済みリリースに移行。 |
| 3.10 | 3.10.6セキュリティアップデート3 |

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、このアドバイザー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やその公表は確認しておりません。

出典

本脆弱性は、シスコ内部でのセキュリティテストによって発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-unauth-infodiscl-LFnLgmey>

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。