# Cisco ADE-OSのローカルファイルインクルージョンの脆弱性

Medium

アドバイザリーID : cisco-sa-ade-xcvAQEOZ
初公開日 : 2021-05-19 16:00
最終更新日 : 2021-06-24 14:24
バージョン 1.2 : Final
CVSSスコア : 4.4
回避策 : No workarounds available
Cisco バグ ID : CSCvw47125 CSCvw48396 CSCvv57166

CVE-2021-1306

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 Evolved Programmable Network(EPN)Manager、Cisco Identity Services Engine(ISE)、およびCisco Prime Infrastructureの制限付きシェルにおける脆弱性により、認証されたローカルの攻撃者がディレクトリを特定し、ファイルシステムに任意のファイルを書き込む可能性があります。

この脆弱性は、制限されたシェル内でCLIコマンドに送信されるパラメータの検証が不適切であることに起因します。攻撃者は、デバイスにログインして特定のCLIコマンドを発行することにより、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、攻撃者は該当デバイスのファイルディレクトリを特定し、任意のファイルを該当デバイスのファイルシステムに書き込むことができます。この脆弱性をエクスプロイトするには、攻撃者が、認証されたシェルユーザーである必要があります。

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-ade-xcvAQEOZ

## 該当製品

### 脆弱性のある製品

この脆弱性の公開時点では、次のシスコ製品とファームウェアリリースに影響を与えていました。

| シスコ製品 | 脆弱性のあるリリース |
|---|---|
| EPNマネージャ | リリース5.0.1より前 |
| ISE | リリース2.6より前のパッチ10<br>リリース2.7より前のパッチ4<br>リリース3.0より前のパッチ2<br>リリース3.1より前 |
| Prime インフラストラクチャ | リリース3.5以降<br>リリース3.9.0より前 |

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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ 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。

## 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、次の表に記載されている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、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

| シスコ製品 | 修正済みリリース |
|---|---|
| EPNマネージャ | 5.0.1 以降 |

| シスコ製品 | 修正済みリリース |
| --- | --- |
| ISE | 2.6 Patch10以降<br>2.7 Patch4以降<br>3.0 Patch2以降<br>3.1 以降 |
| Prime インフラストラクチャ | 3.9.0 以降 |

## 不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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を確認していません。

## 出典

シスコは、この脆弱性を報告していただいたConsciaの従業員に感謝いたします。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ade-xcvAQEOZ

## 改訂履歴

| バージョン | 説明 | セクション | ステータス | 日付 |
| --- | --- | --- | --- | --- |
| 1.2 | Prime Infrastructure 3.8.1アップデート2が公開されていないため、修正として削除されました。 | 「脆弱性のある製品」および「修正済みリリース」 | Final | 2021年6月24日 |
| 1.1 | 脆弱性のある製品および修正済みリリースにISE 2.6 Patch10以降を追加。 | 「脆弱性のある製品」および「修正済みリリース」 | Final | 2021年6月21日 |
| 1.0 | 初回公開リリース | — | Final | 2021 年 5 月 19 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、単独の転載や意訳を施した場合、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。