ReactおよびNext.jsフレームワークのリモートコード実行の脆弱性：2025年12月

アドバイザリーID : cisco-sa-react-flight-TYw32Ddb
初公開日 : 2025-12-04 16:00
最終更新日 : 2025-12-17 22:37
バージョン 1.6 : Final
CVSSスコア : 10.0
回避策 : No workarounds available
Cisco バグ ID :

CVE-2025-55182

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

2025年12月3日、ReactチームはReactサーバの脆弱性CVE-2025-55182に関するセキュリティアドバイザリをリリースしました。これにより、認証されていないリモートの攻撃者が該当デバイスまたはシステムでリモートコードを実行する可能性があります。

この脆弱性の詳細については、public React Security Advisoryを参照してください。

シスコの標準的なプラクティスでは、利用可能になった時点で、統合されたサードパーティ ソフトウェア コンポーネントを新しいバージョンに更新します。

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-react-flight-TYw32Ddb

該当製品

このアドバイザリの「影響を受ける製品」セクションに明示的に記載されていないシスコ製品またはサービスは、記載されている脆弱性の影響を受けません。現在脆弱性が存在しないと判断されている製品は、その後、追加情報が入手可能になり、脆弱性が存在すると判断される可能性があることに注意してください。

脆弱性のある製品

シスコは製品ラインを調査して、この脆弱性により影響を受ける可能性がある製品を特定しました。

脆弱性を含んでいないことが確認された製品

シスコは製品ラインを調査して、この脆弱性により影響を受ける可能性がある製品を特定しました。

本アドバイザリの「脆弱性を含んでいないことが確認された製品」または「脆弱性を含む製品」セクションに記載されていない製品またはクラウドサービスは、脆弱性が存在しないと判断されています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- シスコアプリケーションセントリックインフラストラクチャ(ACI)
- Cisco Finesse

シスコは、この脆弱性が以下のシスコクラウドサービスには影響を与えないことを確認しました。

- AIクラウド
- AppDynamics
- ビジネスクリティカルな洞察
- Catalyst SD-WAN
- Cloud Connectedユニファイドコミュニケーション
- CWAYクラウド
- Crosswork Cloud
- 防衛オーケストレータ
- DevNet、developer.cisco.com
- DevNet Sandbox
- eSIM Flex
- Intersight
- IoT Control Center
- IoT Operations Dashboard
- ISEツール
- 一価
- マネージド サービス アクセラレータ
- マネージドサービスプラットフォーム
- Meraki/ネットワークプラットフォームダッシュボード
- Mobility Mobile Services Core（旧WG2）
- マルチクラウド防御
- Network Based Application Recognition(NBAR)
- ネットワークプラグアンドプレイコネクト、devicehelper.cisco.com
- サービスとしてのプライベート5G
- Provider Connectivity Assurance
- セキュアなアクセス

- Secure Cloud Analytics
- クラウドに関する洞察の保護
- セキュアなEメールクラウドゲートウェイ
- Secure Email Encryptionサービス
- Secure Endpoint
- Cisco Secure Malware Analytics
- Slido
- スマートライセンス
- Smartlook
- Spaces
- Splunkクラウド
- ThousandEyes
- UC Management - Webex発信専用インスタンス
- Unified Communication Managerクラウド
- Vidcast
- Vulnerability Management（旧称：Kenna Security）
- Webex Calling
- Webex発信専用インスタンス
- Webexキャンペーン
- Webex Connect
- Webex Contact Center
- Webex Contact Center Enterprise
- Webexエクスペリエンス管理
- Webex Events
- Webexインタラクション
- Webex Meetings
- Webexメッセージング
- Webex通知
- Webexスイート

回避策

この脆弱性に対処する回避策はありません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-react-flight-TYw32Ddb

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.6	「脆弱性を含んでいないことが確認された製品」のリストと要約セクションを更新。	概要および脆弱性を含んでいないことが確認された製品	Final	2025年12月17日
1.5	脆弱性を含んでいないことが確認された製品のリストを更新。調査に関する文言を修正。	概要および該当製品	Interim	2025年12月11日
1.4	脆弱性を含んでいないことが確認された製品のリストを更新。	脆弱性が存在しない製品	Interim	2025年12月10日
1.3	脆弱性を含んでいないことが確認された製品のリストを更新。	脆弱性が存在しない製品	Interim	2025年12月8日
1.2	脆弱性を含んでいないことが確認された製品のリストを更新。	脆弱性が存在しない製品	Interim	2025年12月6日
1.1	脆弱性を含んでいないことが確認された製品のリストを追加	脆弱性が存在しない製品	Interim	2025年12月5日
1.0	初回公開リリース	—	Interim	2025年12月4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。