ConfD CLI の特権昇格と任意のファイルの読み取り/書き込みにおける脆弱性

アドバイザリーID : cisco-sa-cnfd-rwpesc-ZAOufyx8
初公開日 : 2024-05-15 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No workarounds available
Cisco バグ ID : CSCwj67262 CSCwj72783

CVE-2024-20389
CVE-2024-20326

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

ConfD CLIにおける複数の脆弱性により、認証された低特権のローカル攻撃者が、rootとして任意のファイルの読み取りと書き込みを行ったり、基盤となるオペレーティングシステム上でroot権限に昇格したりする可能性があります。

これらの脆弱性の詳細については本アドバイザリの「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-cnfd-rwpesc-ZAOufyx8

該当製品

脆弱性のある製品

CVE-2024-20326

本脆弱性は ConfD に影響を及ぼします。

脆弱性が存在するConfD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。

CVE-2024-20389

この脆弱性は、ConfDリリース8.0.11に影響を与えます。他のすべてのソフトウェアリリースは影響を受けません。

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、他の脆弱性をエクスプロイトする必要はありません。また、いずれかの脆弱性の影響を受ける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-2024-20326：ConfD の任意ファイルの読み取り/書き込みにおける脆弱性

ConfD CLI の脆弱性により、認証された権限の低いローカルの攻撃者が、基盤となるオペレーティングシステムでルートとして任意のファイルを読み取り/書き込みする可能性があります。

この脆弱性は、特定の CLI コマンド使用時の不適切な認証の適用に起因しています。攻撃者は、細工した引数を指定して影響を受ける CLI コマンドを実行することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者はルートユーザーの権限を使用して基盤となるオペレーティングシステムで任意のファイルを読み取り/書き込みできるようになります。

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：CSCwj67262
CVE ID：CVE-2024-20326
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.8
CVSS ベクトル：CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2024-20389：ConfD の特権昇格の脆弱性

ConfD CLI の脆弱性により、認証された権限の低いローカルの攻撃者が、基盤となるオペレーティングシステムでルートに権限を昇格する可能性があります。

本脆弱性は、特定の CLI コマンド使用時の間違った権限の割り当てに起因しています。攻撃者は、影響を受ける CLI コマンドを実行することで、この脆弱性をエクスプロイトする可能性があり

ます。エクスプロイトに成功すると、攻撃者は基盤となるオペレーティングシステムでルートに権限を昇格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：CSCwj72783
CVE ID：CVE-2024-20389
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.8
CVSS ベクトル：CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

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

シスコのグループ企業である Tail-f は、このアドバイザリに記載された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ました。お客様がインストールしたり、サポートを受けたりできるのは、最新のライセンスを保持し、有効なサポートとメンテナンス契約を持つソフトウェアバージョンとフィーチャセットのみです。当該のソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は Tail-f Systems AB のライセンス条項に従うことに同意したことになります。セキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェアライセンスや追加のソフトウェア フィーチャ セットに対する権限が付与されることはありません。

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。

最新のライセンスを持ち、有効なサポートおよびメンテナンス契約をお持ちのお客様は、既存の Tail-f 配信サーバー ダウンロード アカウントからソフトウェアの修正バージョンをダウンロードできます。

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。情報が明確でない場合は、Tail-f Support システムでサポートチケットを開くことをお勧めします。

修正済みリリース

次の表では、左側の列に ConfD ソフトウェアのリリースが記載されています。中央の列には、脆弱性の影響を受ける最初のリリースが示されています。右側の列には、この脆弱性の修正を含む

リリースが示されています。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。

CVE-2024-20326

ConfD リリース	脆弱性のある最初のリリース	First Fixed Release（修正された最初のリリース）
6.7 以前	脆弱性なし	脆弱性なし
7.1	7.1.7	修正済みリリースに移行。
7.2	7.2.7	修正済みリリースに移行。
7.3	7.3.5	修正済みリリースに移行。
7.4	7.4.5	修正済みリリースに移行。
7.5	7.5.3	7.5.10.2
7.6	7.6	7.6.14.2
7.7	7.7	7.7.15
7.8	7.8	7.8.13.1
8.0	8.0	8.0.12

CVE-2024-20389

ConfD リリース	脆弱性のある最初のリリース	First Fixed Release（修正された最初のリリース）
8.0 以前	脆弱性なし	脆弱性なし
8.0	8.0.11	8.0.12

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とその公表は確認しておりません。

出典

CVE-2024-20326：シスコは、この脆弱性を報告していただいた Elias Ikkelä-Koski 氏に感謝いたします。

CVE-2024-20389：この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cnfd-rwpesc-ZAOufyx8

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 5 月 15 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。