ConfD CLI のセキュアシェルサーバーにおける特権昇格の脆弱性

アドバイザリーID : cisco-sa-confd-priv-esc-LsGtCRx4
CVE-2021-1572
初公開日 : 2021-08-04 16:00
最終更新日 : 2023-10-04 16:00
バージョン 2.0 : Final
CVSSスコア : 7.8
回避策 : No workarounds available
Cisco バグ ID : CSCvy43896 CSCwh35199

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 の脆弱性により、認証されたローカルの攻撃者が、ConfD が実行されているアカウントのレベル（通常は root）で任意のコマンドを実行する可能性があります。この脆弱性を不正利用するには、攻撃者は該当デバイスの有効なアカウントを持っている必要があります。

この脆弱性は、影響を受けるソフトウェアが、CLI の ConfD 組み込みセキュアシェル（SSH）サーバーが有効になっているときに実行していたアカウントの権限レベルで、SFTP ユーザーサービスを誤って実行するために発生します。ConfD 組み込み SSH サーバーが有効になっていない場合、デバイスはこの脆弱性の影響を受けません。低いレベルの権限を持つ攻撃者は、該当デバイスに対して認証を行い、SFTP インターフェイスで一連のコマンドを発行することで、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、ConfD を実行しているアカウントのレベル（通常は root）に権限を昇格させる可能性があります。

注：組み込みのSSHサーバに対して認証できるユーザは、この脆弱性を不正利用する可能性があります。デフォルトでは、サーバーが有効な場合、すべての ConfD ユーザーがこのアクセス権を持ちます。

この脆弱性に対処するソフトウェアアップデートはリリースされています。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-confd-priv-esc-LsGtCRx4

該当製品

脆弱性のある製品

CLI の組み込み SSH サーバーが有効になっている場合、この脆弱性は次のリリースの ConfD に影響します。

- リリース 7.4 ～ 7.4.3
- リリース 7.5 ～ 7.5.2
- リリース 7.6 ～ 7.6.14
- リリース 7.7 ～ 7.7.12
- リリース 7.8 ～ 7.8.10
- リリース 8.0 ～ 8.0.7
- リリース 8.1 ～ 8.1.3

組み込み SSH サーバーが有効になっているかどうかを確認するには、「ConfD and High Security Applications V2」アプリケーションノートのセクション 4.1.1「Disable built-in support for SSH in ConfD」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。ただし、緩和策は使用できます。

管理者は、ConfD 組み込み SSH サーバーを無効にし、OpenSSH などの外部 SSH サーバーを使用できます。ConfD での SSH の組み込みサポートを無効にする方法については、「ConfD and High Security Applications V2 」アプリケーションノートのセクション 4.1.1「Disable built-in support for SSH in ConfD」を参照してください。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

修正済みソフトウェア

Tail-f、シスコ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ています。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、左の列に ConfD ソフトウェアリリースを記載しています。右側の列は、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最初のリリースを示しています。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。

ConfD リリース	First Fixed Release (修正された最初のリリース)
7.4	7.4.3.1
7.5	7.5.2.1
7.6	7.6.14.1
7.7	7.7.13
7.8	7.8.11
8.0	8.0.8
8.1	8.1.4

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

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-confd-priv-esc-LsGtCRx4

改訂履歴

バージョン	説明	セクション	ステータス	日付
2.0	脆弱性のあるリリースおよび修整済リリースに関する情報を更新。	「脆弱性のある製品」および「修正済みリリース」	Final	2023 年 10 月 4 日
1.0	初回公開リリース	—	Final	2021 年 8 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。