複数のシスコ製品での Web ベースの管理インターフェイスの特権昇格における脆弱性

High

アドバイザリーID : cisco-sa-nso-auth-bypass-QnTEesp
初公開日 : 2024-09-11 16:00
最終更新日 : 2024-09-19 16:47
バージョン 1.1 : Final
CVSSスコア : 8.8
回避策 : No workarounds available
Cisco バグ ID : CSCwj31961 CSCwj26769 CSCwj32133

CVE-2024-20381

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 Crosswork Network Services Orchestrator（NSO）、Cisco Optical Site Manager、および Cisco RV340 デュアル WAN ギガビット VPN ルータの Web ベースの管理インターフェイスで使用される ConfD の JSON-RPC API 機能の脆弱性により、認証されたリモート攻撃者が、影響を受けるアプリケーションまたはデバイスの設定を変更する可能性があります。

この脆弱性は、API での不適切な認証チェックに起因します。影響を受けるアプリケーションまたはデバイスにアクセスするのに十分な権限を持つ攻撃者は、JSON-RPC API に悪意のあるリクエストを送信することにより、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、攻撃者は影響を受けるアプリケーションまたはデバイスの設定を不正に変更できる可能性があります。これには、新しいユーザーアカウントを作成したり、影響を受けるシステム上で自分の権限を昇格させたりすることも含まれます。

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-nso-auth-bypass-QnTEesp

該当製品

脆弱性のある製品

この脆弱性は、デバイスの設定に関係なく、次のシスコ製品に影響します。

- Crosswork NSO
- Optical Site Manager
- RV340 デュアル WAN ギガビット VPN ルータ

この脆弱性は、JSON-RPC API 機能が有効になっている場合、ConfD にも影響を与えます。

脆弱性が存在するシスコおよび ConfD ソフトウェアリリースの詳細については、このアドバイザリの「修正済みソフトウェア」の項を参照してください。

ConfD 設定の確認

次の例に示すように、confd.conf 構成ファイルで webui 機能が有効になっている場合、ConfD で JSON-RPC API 機能が有効になります。

```
.
.
.
  <webui>
    <enabled>true</enabled>

    <transport>
      <tcp>
        <enabled>true</enabled>
        <ip>0.0.0.0</ip>
        <port>8008</port>
      </tcp>

      <ssl>
        <enabled>true</enabled>
        <ip>0.0.0.0</ip>
        <port>8888</port>
      </ssl>
    </transport>
     .
     .
     .
</webui>
.
.
.
```

アプリケーション Web サーバーが JSON-RPC 要求を処理するには、ConfD アプリケーションで Web UI 機能が有効になっており、有効なトランスポート（TCP または SSL）と有効なポートが設定されている必要があります。

注：ConfD は独自の Web UI を提供していませんが、XML タグの名前は webui です。examples.confd/json_rpc/webui/README から取られた上記の例は、ポート 8008 および 8888

で JSON-RPC API を有効にする webui の実装を示しています。

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。

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。

- Catalyst SD-WAN コントローラ（旧称、SD-WAN vSmart）
- Catalyst SD-WAN Manager（旧称、SD-WAN vManage）
- Catalyst SD-WAN Validator（旧称、SD-WAN vBond Orchestrator）
- Identity Services Engine（ISE）
- IOS XE SD-WAN ソフトウェア
- SD-WAN vEdge クラウドルータ
- SD-WAN vEdge ルータ

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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

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。

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。

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、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのような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、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意した

ことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ 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、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

この脆弱性の修正済みリリースについては、次の項を参照してください。

confd

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。中央の列は、特定の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ているかどうかを示しています。右側の列は、リリースがこのアドバイザリに記載された脆弱性の影響を受けているかどうか、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	該当するリリース	First Fixed Release（修正された最初のリリース）
7.5	7.5 ~ 7.5.10.1	7.5.10.2
7.7	7.7 ~ 7.7.15	7.7.16
8.0	8.0 ~ 8.0.12	8.0.13

次の表に示すように、該当する修正済みの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。

Crosswork NSO

Cisco Crosswork NSO のリリース	First Fixed Release（修正された最初のリリース）
5.5	5.5.10.1
5.6	5.6.14.3
5.7	5.7.16
5.8	5.8.13.1
6.0	6.0.13
6.1	6.1.8.1 6.1.9
6.2	6.2.3
6.3	影響なし。

Optical Site Manager

Cisco Optical Site Manager リリース	First Fixed Release（修正された最初のリリース）
24.3 より前	修正済みリリースに移行。
24.3	24.3.1

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。

RV340 デュアル WAN ギガビット VPN ルータ

Cisco RV340 デュアル WAN ギガビット VPN ルータについては、このアドバイザリで説明している脆弱性に対応するためのソフトウェアアップデートをリリースしておらず、またリリースする予定もありません。Cisco RV340 デュアル WAN ギガビット VPN ルータは、サポート終了プロセスに入っています。お客様には、これらの製品のサポート終了通知を参照することをお勧めします。

Cisco RV 160、RV260、RV345P、RV340W、RV260W、RV260P、および RV160W VPN ルータの販売終了およびサポート終了のお知らせ

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-nso-auth-bypass-QnTEesp

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	設定例を修正。	脆弱性が存在する製品	Final	2024年9月19日
1.0	初回公開リリース	—	Final	2024 年 9 月 11 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。