Cisco Crosswork Network Services Orchestratorの脆弱性

アドバイザリーID : cisco-sa-nso-rwpesc-qrQGnh3f
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 : CSCwi84310 CSCwi31715

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

Cisco Crosswork Network Services Orchestrator(NSO)CLIの複数の脆弱性により、認証された権限の低いローカルの攻撃者が、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-nso-rwpesc-qrQGnh3f

該当製品

脆弱性のある製品

これらの脆弱性は、Cisco Crosswork NSOに影響を与えます。

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。

Cisco Crosswork NSOが各脆弱性によってどのように影響されるかについては、次のセクションを参照してください。

CVE-2024-20326

Cisco Crosswork NSOは、次の条件の1つ以上に当てはまる場合にのみ、CVE-2024-20326で説明されている脆弱性の影響を受けます。

- デバイスで、修正されたncs.ccl CLI仕様ファイル(clispec)が実行されている。
- デバイスは、インストール時に提供されるncs.cclクリスペックを実行していません。
- ユーザは、基盤となるオペレーティングシステムでCisco Crosswork NSO Network Simulator(Netsim)を実行できます。

注：ユーザがNetsimツールを実行できる場合、デバイスはclispecステータスに関係なく影響を受けます。

Netsimツールの詳細については、Cisco Crosswork NSOのドキュメントの「ネットワークシミュレータ」のセクションを参照してください。

デバイスでncs.cclクリスペックが実行されているかどうかを確認する

Cisco Crosswork NSOでは、デフォルトのclispec(ncs.ccl)をカスタマイズできます。デバイスで修正されたncs.cclクリスペックが実行されているか、ncs.cclクリスペックが削除されているか、ncs.cclクリスペックがデバイスで設定されていない場合、そのデバイスは影響を受けます。

ncs.cclクリスペックがデバイスで実行されているかどうかを確認するには、次の例に示すように、describe pingコマンドを使用します。

```
<#root>

admin@ncs>

describe ping


Common


Source : clispec
    File   : /opt/ncs/ncs-6.2.4/etc/ncs/ncs.ccl


Callback [os command]
.
.
.
```

コマンドがclispecのソース値と<nso installation dir>/etc/ncs/ncs.cclのファイル値を返す場合、

デバイスはncs.ccl clispecを実行しています。ncs.cclクリスペックを調べて、修正されているかどうかを確認します。

describe pingコマンドを実行して、前の例と異なるSourceまたはFileの値を出力した場合、そのデバイスは影響を受け、それ以上のチェックは必要ありません。次の例は、該当デバイスからの出力を示しています。

```
<#root>

admin@ncs>

describe ping


Common


Source : built-in


Callback [os command]
.
.
.
```

ncs.cclクリスペックが変更されているかどうかを確認する

管理者がncs.ccl clispecを変更したかどうかを判断するには、次の例に示すように、sourceディレクトリからshasum -a 256 ncs.cliコマンドを使用して、ncs.cli clispecソースファイルのハッシュを計算します。

```
<#root>

<nso_installation_path>/src/ncs/cli/

shasum -a 256 ncs.cli

1bbcf2ec885311eed22a21644cbe02c211ee45e8a4ff2be56769324534a26f0d  ncs.cli
```

返されたハッシュ値が前の例と正確に一致する場合、ソースファイルは変更されていません。

CVE-2024-20389

Cisco Crosswork NSOリリース6.0.11および6.2.1のみが、CVE-2024-20389で説明されている脆弱性の影響を受けます。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:Cisco Crosswork NSOにおける任意ファイルの読み書きの脆弱性

Cisco Crosswork NSO 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の読み取りおよび書き込みを行う可能性があります。

この脆弱性は、特定のCLIコマンドを使用した際の不適切な許可の適用に起因します。攻撃者は、巧妙に細工された引数を含む特定のCLIコマンドを使用することで、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rootレベルの権限を使用して、基盤となるオペレーティングシステム上で任意のファイルの読み取りまたは書き込みを行え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:CSCwi31715
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:Cisco Crosswork NSOの権限昇格の脆弱性

Cisco Crosswork NSO CLIの脆弱性により、認証された低特権のローカル攻撃者が、基盤となるオペレーティングシステムでルートとして特権を昇格できる可能性があります。

この脆弱性は、特定のCLIコマンドを使用した際の不適切な権限割り当てに起因します。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、基盤となるオペレーティングシステムでルートとして特権を昇格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:CSCwi84310
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。

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

次の表では、左の列にシスコソフトウェアリリーストレインを示します。中央の列には、このアドバイザリに記載された脆弱性の影響を受ける各トレインの最初のリリースを示します。 右の列は、これら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。

CVE-2024-20326

Cisco Crosswork NSOリリース	影響を受ける最初のリリース	First Fixed Release (修正された最初のリリース)
4.7 以前	脆弱性なし	脆弱性なし
5.1	5.1.7	修正済みリリースに移行。
5.2	5.2.7	修正済みリリースに移行。
5.3	5.3.5	修正済みリリースに移行。
5.4	5.4.5	修正済みリリースに移行。
5.5	5.5.3	5.5.10.1
5.6	5.6	5.6.14.3
5.7	5.7	5.7.15
5.8	5.8	5.8.13.1
6.0	6.0	6.0.12
6.1	6.1	6.1.7
6.2	6.2	6.2.2
6.3	脆弱性なし	脆弱性なし

CVE-2024-20389

Cisco Crosswork NSOリリース	影響を受ける最初のリリース	First Fixed Release（修正された最初のリリース）
7.8 以前	脆弱性なし	脆弱性なし
6.0	6.0.11	6.0.12
6.1	N/A	脆弱性なし
6.2	6.2.1	6.2.2
6.3	脆弱性なし	脆弱性なし

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

CVE-2024-20326：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-nso-rwpesc-qrQGnh3f

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

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。