Cisco Routedパッシブ光ネットワークコントローラの脆弱性

High

アドバイザリーID : cisco-sa-iosxr-ponctlr-ci-OHcHmsFL
初公開日 : 2024-09-11 16:00
バージョン 1.0 : Final
CVSSスコア : 8.4
回避策 : No workarounds available
Cisco バグ ID : CSCwi81013 CSCwi81012 CSCwi81017

CVE-2024-20489
CVE-2024-20483

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 IOS XRソフトウェアでサポートされているハードウェア上でDockerコンテナとして実行されるCisco Routed Passive Optical Network(PON)コントローラソフトウェアの複数の脆弱性により、認証されたリモート攻撃者がコマンドインジェクション攻撃を実行したり、該当システムで任意のコマンドを実行したり、クリアテキストのパスワードを取得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。

シスコでは、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する予定です。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-iosxr-ponctlr-ci-OHcHmsFL

このアドバイザリは、2024年9月に公開されたCisco IOS XRソフトウェアセキュリティアドバイザリバンドルの一部です。アドバイザリとリンクの一覧については、Cisco Event Response: September 2024 Semiannual Cisco IOS XR Software Security Advisory Bundled Publication を参照してください。

該当製品

脆弱性のある製品

これらの脆弱性は、Cisco IOS XRソフトウェアの脆弱性が存在するリリースを実行し、ルーテッドPONコントローラ機能が設定されている次のシスコハードウェアプラットフォームに影響を与えます。

Network Convergence System（NCS）540 シリーズ ルータ

- NCS 540-24Q8L2DD-SYSルータ
- NCS 540-24Z8Q2C-SYSルータ
- NCS 540-28Z4C-SYS-Aルータ
- NCS 540-28Z4C-SYS-Dルータ
- NCS 540-ACC-SYSルータ
- NCS 540X-16Z4G8Q2C-Aルータ
- NCS 540X-16Z4G8Q2C-Dルータ

NCS 5500 シリーズ

- NCS 55A1-24Q6H-SS
- NCS 55A2-MOD-SE-S

NCS 5700 シリーズ

- NCS-57C1-48Q6-SYS
- NCS 57C3-MOD

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 PONコントローラソリューションの詳細については、『Ciscoルーテッドパッシブ光ネットワーク導入ガイド』を参照してください。

PONコントローラソフトウェアが有効になっているかどうかの確認

Cisco IOS XRソフトウェアでPONコントローラが有効になっているかどうかを確認するには、該当するデバイスのCLIでshow running-config pon-ctlrコマンドを使用します。次の例に示すように、コマンドがデバイスにPONコントローラが設定されていることを示す出力を返す場合、デバイスはこれらの脆弱性の影響を受けます。

<#root>

```
RP/0/RP0/CPU0:Router#
show running-config pon-ctrl

Wed Sep 11 03:00:53.842 UTC
```

```
pon-ctlr


cfg-file harddisk:/PonCntlInit.json vrf default
RP/0/RP0/CPU0:Router#
.
.
.
```

出力が空の場合、またはコマンドが存在しない場合、デバイスはこれらの脆弱性の影響を受けません。

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。

シスコは、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- IOS ソフトウェア
- IOS XE ソフトウェア
- NX-OS ソフトウェア

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別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェア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-2024-20483:CiscoルーテッドPONコントローラコマンドインジェクションの脆弱性

Cisco IOS XRソフトウェアでサポートされているハードウェア上のDockerコンテナとして実行されるCiscoルーテッドPONコントローラソフトウェアの複数の脆弱性により、PONマネージャの管理者レベルの権限を持つ、またはPONマネージャのMongoDBインスタンスへの直接アクセスを持つ認証されたリモート攻撃者が、PONコントローラコンテナに対するコマンドインジェクション攻撃を実行し、rootとして実行実行します。

これらの脆弱性は、特定のコンフィギュレーションコマンドに渡される引数の検証が不十分であることに起因します。攻撃者は、該当のコンフィギュレーションコマンドの引数として巧妙に細工された入力を含めることによって、これら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PONコントローラでrootとして任意のコマンドを実行できる可能性があります。

シスコでは、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する予定です。これらの脆弱性に対処する回避策はありません。

バグID: CSCwi81012、CSCwi81013
CVE ID：CVE-2024-20483
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.2
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVE-2024-20489:Cisco Routed PONコントローラのクリアテキストパスワードの脆弱性

PONコントローラコンフィギュレーションファイルのストレージ方式の脆弱性により、権限の低い認証されたローカル攻撃者がMongoDBクレデンシャルを取得できる可能性があります。

この脆弱性は、Cisco IOS XRソフトウェアを実行しているデバイスに、暗号化されていないデータベースのクレデンシャルが不適切に保存されることに起因します。攻撃者は、該当システムのコンフィギュレーションファイルにアクセスすることで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はMongoDBクレデンシャルを表示できる可能性があります。

シスコでは、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する予定です。この脆弱性に対処する回避策はありません。

バグID:CSCwi81017
CVE ID：CVE-2024-20489
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：8.4
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N

回避策

これらの脆弱性に対処する回避策はありません。ただし、管理者は、PONマネージャと各Cisco IOS XRソフトウェアPONコントローラのIPアドレスへのMongoDBアクセスを制限できます。これらの制限の実装については、MongoDBのドキュメント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

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提供する

予定です。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またはトレインを示します。右の列は、リリース（トレイン）がこのアドバイザリに記載された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。

Cisco IOS XR[1]のCiscoルーテッドPONコントローラソフトウェア	First Fixed Release（修正された最初のリリース）
7.11 以前	脆弱性なし
24.1 以降	修正済みリリースに移行。
24.2 以降	修正済みリリースに移行。
24.3 以降	修正済みリリースに移行。
24.4.1 (Nov 2024)	脆弱性なし

1. CiscoルーテッドPONコントローラソフトウェアは、オプションのRPMパッケージマネージャとしてCisco IOS XRソフトウェアにバンドルされています。

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。

修正済みソフトウェアにアップグレードした後、キーリングを使用してMongoDBパスワードを保存するには、 PonCntlInit.jsonファイルで設定を変更する必要があります。

PonCntlInit.json構成変更の手順

修正済みソフトウェアにアップグレードした後、次の例に示すように、 PonCntlInit.jsonファイルのMongoDBパスワードフィールドを password_optsフィールドで置き換えます。

設定を変更する前に、次の例に示すようにMongoDBパスワードフィールドが表示されます。

<#root>

```
"MongoDB": {
        "auth_db": "tibit_users",
.
.
.
.

"password"

: "MongoDBPassword",
.
.
}
```

修正済みソフトウェアにアップグレードした後、次の例に示すように、MongoDBのpasswordフ

ィールドをpassword_optsフィールドで置き換えます。

<#root>

```
"MongoDB": {
.
.
.
"
```

password_opts

```
": {
```

"type": "keyring",

"keyring_path": "/etc/cisco/poncntl/keyring.data",

"keyring_key_path": "/etc/cisco/poncntl/keyring.key"

```
},
.
.
}
```

PonCntlInit.jsonファイルを編集したら、Cisco IOS XRソフトウェアの設定を更新して、データベースパスワードを含めます。設定を保存すると、show running-configコマンドを実行したときにパスワードが暗号化形式で表示されます。次に例を示します。

<#root>

```
Router#conf t
Wed Sep 11 16:00:00.000 UTC
Router(config)#pon-ctlr
Router(config-ponctlr)#
```

cfg-file /harddisk:/PonCntlInit.json db-password

```
Router(config-ponctlr)#end
RP/0/RP0/CPU0:Sep 11 16:00:00.000 UTC: config[67636]: %MGBL-SYS-5-CONFIG_I : Configured from console by
Router#
```

show running-config pon-ctlr

```
Wed Sep 11 16:00:00.000 UTC
pon-ctlr
 cfg-file /harddisk:/PonCntlInit.json
```

```
db-password
 0525253C1E6E6925
!
Router#
```

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

これらの脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のJames Spadaroによる社内セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-ponctlr-ci-OHcHmsFL

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。