複数のシスコ製品における CLI コマンドインジェクションの脆弱性

High

アドバイザリーID : cisco-sa-cli-cmdinj-4MttWZPB
初公開日 : 2022-01-19 16:00
バージョン 1.0 : Final
CVSSスコア : 8.8
回避策 : No workarounds available
Cisco バグ ID : CSCvz49669 CSCvq58164 CSCvq22323 CSCvq58183 CSCvq21764 CSCvq58204 CSCvq58226 CSCvq58224 CSCvq58168 CSCvm76596

CVE-2022-20655

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

複数のシスコ製品で使用されている CLI の実装に存在する脆弱性により、認証されたローカル攻撃者がコマンドインジェクション攻撃を実行する可能性があります。

この脆弱性は、該当製品でプロセス引数の検証が十分に行われないことに起因します。攻撃者は、このプロセスの実行中にコマンドインジェクションを実行することにより、この脆弱性をエクスプロイトする可能性があります。攻撃者がエクスプロイトに成功すると、一般的にルート権限である管理フレームワークプロセスの権限で、基盤となるオペレーティングシステムに対して任意のコマンドが実行される危険性があります。

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。

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-cli-cmdinj-4MttWZPB

該当製品

シスコでは、この脆弱性の影響を受ける製品およびサービスを判断するために、製品ラインを調査しました。このアドバイザリの「修正済みソフトウェア」のセクションで、影響を受ける各製品またはサービスの Cisco Bug ID を示します。Cisco Bug は Cisco Bug Search Tool で検索可能

であり、プラットフォーム固有の追加情報と修正されたソフトウェアリリースが記載されます。

本アドバイザリの「脆弱性のある製品」セクションに記載されていない製品またはサービスは、脆弱性が存在しないと判断されています。

脆弱性のある製品

この脆弱性は、脆弱なソフトウェアリリースを実行している次の製品に影響を及ぼします。

モバイル インターネット

- Cisco Ultra Gateway Platform

ネットワーク管理とプロビジョニング

- Cisco Enterprise NFV Infrastructure Software（NFVIS）
- Cisco Network Services Orchestrator（NSO）
- Cisco Virtual Topology System（VTS）

オプティカル ネットワーク

- Cisco Carrier Packet Transport[1]

Routing and Switching - Enterprise and Service Provider

- Cisco SD-WAN vBond ソフトウェア
- Cisco SD-WAN vEdge ルータ
- Cisco SD-WAN vManage ソフトウェア
- Cisco SD-WAN vSmart ソフトウェア
- Cisco IOS XE SD-WAN
- Cisco IOS XR（64 ビット）ソフトウェア

1. Cisco Carrier Packet Transport のサポートは終了しました。

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。

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製品およびサービスには影響を与えないことを確認しました。

クラウドおよびシステム管理

- Cisco Evolved Programmable Network Manager

- Cisco Prime Network Registrar

ネットワーク アプリケーション、サービス、およびアクセラレーション

- Cisco Cloud Services Platform 2100
- Cisco Wide Area Application Services（WAAS）

ネットワーク管理とプロビジョニング

- Cisco Data Center Network Manager
- Cisco Elastic Services Controller
- Cisco NetFlow Generation Appliance
- Cisco Network Analysis Module
- Cisco Virtual Topology Service Routing（VTSR）
- Cisco Virtual Topology Forwarder（VTF）

オプティカル ネットワーク

- Cisco Network Convergence System（NCS）2000 シリーズ Shelf Virtualization Orchestrator（SVO）

Routing and Switching - Enterprise and Service Provider

- Cisco IOS ソフトウェア
- Cisco IOS XE ソフトウェア
- Cisco IOS XR（32 ビット）ソフトウェア
- Cisco NX-OS ソフトウェア

ルーティングおよびスイッチング - スモール ビジネス

- Cisco RV160 VPN ルータ
- Cisco RV160W Wireless-AC VPN ルータ
- Cisco RV260 VPN ルータ
- PoE 対応 Cisco RV260P VPN ルータ
- Cisco RV260W Wireless-AC VPN ルータ
- Cisco RV340 デュアル WAN ギガビット VPN ルータ
- Cisco RV340W デュアル WAN ギガビット Wireless-AC VPN ルータ
- Cisco RV345 デュアル WAN ギガビット VPN ルータ
- Cisco RV345P デュアル WAN ギガビット PoE 対応 VPN ルータ

サーバ：ユニファイド コンピューティング

- Cisco Integrated Management Controller

音声およびユニファイド コミュニケーション デバイス

- Cisco Unified Communications Manager Session Management Edition
- Cisco Unified Communications Manager

ワイヤレス

- Cisco Mobility Services Engine

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。

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 Cisco Support and Downloads 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。

シスコ製品	Cisco Bug ID	First Fixed Release（修正された最初のリリース）
モバイル インターネット		
Ultra Gateway Platform	CSCvz49669	6.15.0
ネットワーク管理とプロビジョニング		
エンタープライズ NFV インフラストラクチャ ソフトウェア（NFVIS）	CSCvm76596	3.12.1
Network Services Orchestrator（NSO）	CSCvq22323	4.3.9.1、4.4.5.6、4.4.8、4.5.7、4.6.1.7、4.6.2、4.7.1、5.1.0.1、5.2
Virtual Topology System (VTS)	CSCvq58164	2.6.5
オプティカル ネットワーク		
Carrier Packet Transport	CSCvq58204	ソフトウェアメンテナンスは終了しました。公開済みの修正プログラムはありません.次の項を参照してください。
Routing and Switching - Enterprise and Service Provider		
IOS XE SD-WAN	CSCvq58224	16.10.2、16.12.1b、17.2.1r
IOS XR（64 ビット）ソフトウェア	CSCvq58168	7.0.2, 7.1.1
Network Convergence System（NCS）4009、4016	CSCvq58183	6.5.32（2022 年 1 月）
SD-WAN vBond ソフトウェア	CSCvq58226	18.4.4、19.2.1、19.3.0、20.1.1
SD-WAN vEdge ルータ	CSCvq58226	18.4.4、19.2.1、19.3.0、20.1.1
SD-WAN vManage ソフトウェア	CSCvq58226	18.4.4、19.2.1、19.3.0、20.1.1
SD-WAN vSmart ソフトウェア	CSCvq58226	18.4.4、19.2.1、19.3.0、20.1.1

Cisco Carrier Packet Transport (CSCvq58204)

Cisco Carrier Packet Transport はサポート終了プロセスに入っているため、シスコはこの製品の脆弱性に対処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、今後もリリースする予定はありません。お客様には、こ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 Carrier Packet Transport の販売終了とサポート終了のご案内

デバイスの移行を検討する際は、[シスコ セキュリティ アドバイザリ (Cisco Security Advisories)] 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の有無と完全なアップグレード ソリューションを確認してください。

いずれの場合も、お客様は新しいデバイスがネットワークのニーズに十分に対応でき、十分なメモリがあり、現在のハードウェアおよびソフトウェア構成が新しい製品で引き続き適切にサポートされることを確認する必要があります。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。

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

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-cli-cmdinj-4MttWZPB

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	2022 年 1 月 19 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。