Cisco IOS XEソフトウェアのDECnetフェーズIV/OSIにおけるサービス妨害(DoS)の脆弱性

High

アドバイザリーID : cisco-sa-iosxe-decnet-dos-cuPWDkyL

CVE-2021-1352

初公開日 : 2021-03-24 16:00

バージョン 1.0 : Final

CVSSスコア : 7.4

回避策 : No workarounds available

Cisco バグ ID : CSCvv51476

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 XEソフトウェアのDECnet Phase IVおよびDECnet/OSIプロトコル処理における脆弱性により、認証されていない隣接する攻撃者が、該当デバイスでサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、該当デバイスが受信するDECnetトラフィックの入力検証が不十分であることに起因します。攻撃者は、該当デバイスにDECnetトラフィックを送信することで、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、攻撃者は該当デバイスのリロードを引き起こし、その結果DoS状態が発生す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ました。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、次のリンクで確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-decnet-dos-cuPWDkyL

このアドバイザリは、Cisco IOSおよびIOS XEソフトウェアセキュリティアドバイザリバンドル公開の2021年3月リリースの一部です。これらのアドバイザリとリンクの完全なリストについては、「Cisco Event Response:Cisco IOSおよびIOS XEソフトウェアに関するセキュリティアドバイザリ公開資料（半年刊、2021年3月）

該当製品

脆弱性のある製品

この脆弱性は、Cisco IOS XEソフトウェアの脆弱性のあるリリースを実行し、DECnet Phase IVまたはDECnet/OSIプロトコルが有効になっているシスコデバイスに影響を与えます。DECnetはデフォルトでは有効になっていません。

脆弱性が存在するシスコ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。

デバイス設定の確認

DECnetが有効になっているかどうかを確認するには、**show decnet interfaceコマンドを使用**します。次の例は、GigabitEthernet0/0/0インターフェイスでDECnetが設定されているデバイスの出力を示しています。

```
router# show decnet interface
.
.
.
GigabitEthernet0/0/0 is up, line protocol is up, encapsulation is ARPA
 Interface cost is 1, priority is 64, DECnet network: 0
 We are the designated router
 Sending HELLOs every 15 seconds, routing updates 40 seconds
.
.
.
```

DECnet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。**show decnet interfaceコマンドの次の出力例を参照**してください。

```
router#show decnet interface
% DECnet is not enabled
```

さらに、**show decnet interfaceコマンドの次の出力例に示すように、すべてのインターフェイスでDECnetプロトコル処理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。**

```
router#show decnet interface
.
.
. GigabitEthernet0/0/0 is up, line protocol is up, encapsulation is ARPA
DECnet protocol processing not enabled
.
.
.
```

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確認されています。

シスコは、この脆弱性が次のシスコ製品には影響を与えないことを確認しました。

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

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ている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ました。お客様は、ライセンスを購入したソフトウェアバージョンおよびフィーチャセットのインストールとサポートの予定のみを行うことができます。こ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することにより、お客様はシスコソフトウェアライセンスの条項に従うことに同意します。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様は、有効なライセンスを持っているソフトウェアのみをダウンロードできます。このソフトウェアは、シスコから直接、またはシスコ認定リセラーまたはパートナーを通じて調達されます。ほとんどの場合、これは以前に購入したソフトウェアへのメンテナンスアップグレードになります。無償のセキュリティソフトウェアアップデートでは、新しいソフトウェアライセンス、追加のソフトウェア機能セット、またはメジャーリビジョンのアップグレードを利用できません。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisoriesページから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、問題の有無と完全なアップグレードソリューションを確認することをお勧めします。

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搭載されていることを確認し、現在のハードウェアおよびソフトウェアの設定が新しいリリース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。情報が明確でない場合は、Cisco Technical Assistance Center(TAC)または契約しているメンテナンスプロバイダーにお問い合せください。

サービス契約をお持ちでないお客様

シスコから直接購入し、シスコのサービス契約を締結していないお客様、およびサードパーティベンダーを通じて購入したが、販売時点で修正済みソフトウェアを入手できない場合は、Cisco TACに連絡してアップグレードを入手してください。

https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

お客様は製品シリアル番号を入手し、無料アップグレードの資格を証明するためにこのアドバイザリのURLを提供できるように準備する必要があります。

Cisco IOSおよびIOS XEソフトウェア

お客様がCisco IOSおよびIOS XEソフトウェアの脆弱性に該当するかどうかを判断できるように、Cisco Software Checkerを使用して、特定のソフトウェアリリースに影響するCisco Security Advisoryと、各アドバイザリに記載されている脆弱性を修正した最初のリリース(「First Fixed」)をです。 該当する場合、このツールは、特定されたすべてのアドバイザリに記載されているすべての脆弱性を修正した最初のリリース(「Combined First Fixed」)も返します。

お客様は、Cisco Software Checkerを使用して次の方法でアドバイザリを検索できます。

- ソフトウェアと1つ以上のリリースを選択します
- 特定のリリースのリストを含む.txtファイルをアップロードします
- **show version**コマンドの出力**を入力します**

検索を開始した後、すべてのCisco Security Advisories、特定のアドバイザリ、または最新のバンドル公開のすべてのアドバイザリを含むように検索をカスタマイズできます。

また、次のフォームを使用して、Cisco IOSまたはIOS XEソフトウェアリリース(**15.1(4)M2**や**3.13.8Sなど)を入力して、リリースがCisco Security Advisoryの影響を受けるかどうかを確認できます。**

デフォルトでは、Cisco Software Checkerには、CriticalまたはHigh Security Impact Rating(SIR)を持つ脆弱性の結果のみが含まれます。 Medium SIRの脆弱性の結果を含めるには、Cisco.comのCisco Software Checkerを使用し、検索をカスタマイズするときに**Impact Ratingのドロップダウンリストの**Mediumチェックボックスをオンにします。

Cisco IOS XEソフトウェアリリースとCisco IOSソフトウェアリリースのマッピングについては、Cisco IOS IOSに応じて、Cisco IOS XE 2リリースノート、Cisco IOS XE 3Sリリースノート、またはCisco IOS XE 3SGリリースノートを参照してくださいXEソフトウェアリリース

不正利用事例と公式発表

Cisco Product Security Incident Response Team(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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-decnet-dos-cuPWDkyL

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	最初のパブリックリリース。	—	最終	2021年3月24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。