

Cisco Virtualized Packet Core-Distributed Instance Denial of Service Vulnerability

High

アドバイザリーID : cisco-sa-20180207-vpcdi

初公開日 : 2018-02-07 16:00

バージョン 1.0 : Final

CVSSスコア : [8.6](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCve17656](#)

[CVE-2018-0117](#)

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 Virtualized Packet Core-Distributed Instance (VPC-DI) ソフトウェアの入力パケット処理機能における脆弱性により、認証されていないリモート攻撃者が該当システムの制御機能 (CF) の両方のインスタンスをリロードし、Denial of Service (DoS) 状態を発生させる可能性があります。

この脆弱性は、該当ソフトウェアによるユーザ入力データ処理が不十分であることに起因します。この脆弱性は、悪意のあるトラフィックが該当システムの内部分散インスタンス (DI) のネットワークアドレスに送信されることで、エクスプロイトされる可能性があります。エクスプロイトに成功すると、該当システム上で処理されないエラー状態が引き起こされて CF インスタンスのリロード (さらに VPC 全体のリロード) が発生し、すべてのサブスクライバが切断され、システムが DoS 状態に陥る可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

このアドバイザリーは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-vpcdi>

該当製品

脆弱性のある製品

この脆弱性は、最初の修正済みリリース前の Cisco StarOS オペレーティング システムのすべ

てのリリースを実行する Cisco Virtualized Packet Core-Distributed Instance (VPC-DI) ソフトウェアに影響を与えます。

Cisco StarOS の脆弱なリリースが VPC-DI 例で動作しているかどうか判別するために、管理者はデバイス CLI で **show version** コマンドを使用できます。次の例は、Cisco StarOS リリース 19.3.v5 (VPC-DI リリース N4.2.5) を実行している VPC-DI インスタンスに対してコマンドを実行した結果を示しています。それぞれ VPC-DI および Cisco StarOS ソフトウェア両方のすべてのメジャーリリースをリストする **修正済みソフトウェアのセクション**の表を参照して下さい。

```
[local]VPC-001# show version

Active Software:
Image Version: 19.3.v5
Image Build Number: 65002
Image Description: Deployment_Build
Image Date: Wed Sep 14 05:35:14 EDT 2016
Boot Image: /flash/qvpc-di-19.3.v5.bin
```

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

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。

- Virtualized Packet Core-Single Instance (VPC-SI) ソフトウェア
- ASR 5000
- Elastic Services Controller
- Ultra Automation Services

詳細

DI ネットワークは VPC-DI インスタンスの仮想マシン (VM) と相互接続して、VM が相互に通信することを可能にします。DI ネットワークは、単一 VPC-DI インスタンスの排他的使用のために予約された固有の分離したネットワークにする必要があります。その他のデバイスを DI ネットワークに接続しないでください。1つのデータセンターで複数の VPC-DI インスタンスをインスタンス化する場合は、各インスタンスに独自の DI ネットワークが必要です。

この脆弱性をエクスプロイトするには、攻撃者が IPv4 で VPC-DI インスタンスの DI ネットワークインターフェイスに TCP パケットを送信する必要があります。

脆弱なコードは VPC-DI ソフトウェアにのみ存在します。この脆弱性は、Cisco VPC-SI ソフトウェア、および「脆弱性が存在しない製品」の項に掲載された他のシスコ製品には存在しません。

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 アップデートを提供しています。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、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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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です。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。

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 and Alerts 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、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 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>

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

次の表の左の列には、Cisco VPC-DI ソフトウェアのメジャー リリースを、中央の列には Cisco StarOS のメジャー リリースをそれぞれ記載しています。右の列は、メジャー リリースが本アドバイザリに記載している脆弱性に該当するかどうか、また、本脆弱性に対する修正を含む最初のマイナー リリースに該当するかどうかを示します。

次の表に示すように、適切なリリースにアップグレードする必要があります。

Cisco VPC-DI メジャーリリース	Cisco StarOS Major Release	Ciscoバグ CSCve17656 のための修正済みリリース
N4.0	19.2	影響あり。 N5.1.9 (21.1.v7) への移行が必
N4.2	19.3	影響あり。 N5.1.9 (21.1.v7) への移行が必
N4.5	20.0	影響あり。 N5.1.9 (21.1.v7) への移行が必
N4.6	20.1	影響あり。 N5.1.9 (21.1.v7) への移行が必
N4.7	20.2	影響あり。 N5.1.9 (21.1.v7) への移行が必
N5.0	21.0	影響あり。 N5.1.9 (21.1.v7) への移行が必
N5.1	21.1	N5.1.9 (21.1.v7)
N5.5	21.3	N5.5.0 (21.3.v10)

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エクスプロイト事例やその公表を確認していません。

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-vpcdi>

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-February-07

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、単独の転載や意識を施した場合、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。