Cisco Virtualized Packet Core-Distributed Instance Denial of Service Vulnerability

High

アドバイザリーID : cisco-sa-20170621-vpc
初公開日 : 2017-06-21 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : Yes
Cisco バグ ID : CSCvc01665 , CSCvc35565

CVE-2017-6678

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 UDP パケット処理機能の脆弱性により、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にリロードを引き起こし、サービス妨害（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。 攻撃者はこの脆弱性をエクスプロイトして、両方の CF インスタンスの分散インスタンス（DI）ネットワーク アドレスに、巧妙に細工された UDP パケットを送信す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。

この脆弱性のエクスプロイトは、IPv4 トラフィックでのみ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、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-vpc

影響を受ける製品

脆弱性が存在する製品

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。 以下に、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 インスタンスでのコマンド出力例を示します。

```
[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
```

脆弱性が存在しない製品

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 シリーズ アグリゲーション サービス ルータ [英語]
- Elastic Services Controller
- Ultra Automation Services

細部

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 経由で 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 UDP パケットを送信できる必要があります。

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。

固定ソフトウェア

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。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.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。

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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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。
http://www.cisco.com/c/ja_jp/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

次の表では、最初の列に Cisco VPC-DI ソフトウェアのメジャー リリース、およびカッコ内に関連付けられた Cisco StarOS オペレーティング システムのリリースを示します。 2 列目と 3 列目は、この脆弱性に関連付けられた Cisco Bug に対する修正を含む最初のマイナー リリースを示します。 4 列目は、この脆弱性に対処するためにインストールを推奨するリリースを示します。

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 Software and Cisco StarOS メジャー リリース	First Fixed Release for Cisco Bug CSCvc01665	First Fixed Release for Cisco Bug CSCvc35565	推奨リリ
N4.0 (19.2)	N4.2.6 (19.3.v6)	N4.2.7 (19.3.v7)	N4.2.7 (19.3.v7) later
N4.2 (19.3)	N4.2.6 (19.3.v6)	N4.2.7 (19.3.v7)	N4.2.7 (19.3.v7) later
N4.5 (20.0)	N4.7.2 (20.2.v2)	N4.7.2 (20.2.v2)	N4.7.2 (20.2.v2) later
N4.6 (20.1)	N4.7.2 (20.2.v2)	N4.7.2 (20.2.v2)	N4.7.2 (20.2.v2) later
N4.7 (20.2)	N4.7.2 (20.2.v2)	N4.7.2 (20.2.v2)	N4.7.2 (20.2.v2) later
N5.0 (21.0)	Not affected	N5.1 (21.1.v0)	N5.1 (21.1.v0) later
N5.1 (21.1)	Not affected	Not affected	Not affec

アクティブなサービス サービス契約を持つ顧客は Cisco ファイル Exchange からの修正済みソフトウェアリリースをダウンロードできます。

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。

ソース

本脆弱性はお客様のサポート 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-20170621-vpc

改訂履歴

Version	Description	Section	Status	Date
1.0	Initial public release.		Final	2017-June-21

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。