

サービス拒否の脆弱性を処理する Cisco IOS および Cisco IOS XE ソフトウェア UDP パケット

Medium	アドバイザーID : cisco-sa-20170906-ios-udp	CVE-2017-6627
m	初公開日 : 2017-09-06 16:00	
	最終更新日 : 2017-09-07 13:35	
	バージョン 1.1 : Final	
	CVSSスコア : 5.3	
	回避策 : Yes	
	Cisco バグ ID : CSCva95506 , CSCve64219 , CSCup10024	

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 のコードおよび Cisco IOS XE ソフトウェアを処理する UDP の脆弱性は非認証、リモート攻撃者により影響を受けたシステムのインพุットキューは UDP パケットが保持されますことを可能にする可能性があります。インターフェイスキュー ウェッジおよびサービス拒否 (DoS) 状態を引き起こします。

脆弱性は UDP ソケットを作成し、それらを閉じないでソケット アイドル状態を残す Cisco IOS ソフトウェア アプリケーション変更が原因です。攻撃者は影響を受けたデバイスへの宛先ポートが付いている UDP パケットを送信することによってこの脆弱性を不正利用する可能性があります。正常なエクスプロイトは攻撃者が UDP パケットを DoS 状態に終ってインพุットインターフェイス キューで、保持されますことを可能にする可能性があります。インพุットインターフェイス キューは 250 のパケットを受信する場合 UDP パケットが保持されることを止めます。

この脆弱性に対処する回避策があります。

このアドバイザーは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170906-ios-udp>

該当製品

修正済みソフトウェア

この脆弱性は Cisco IOS および Cisco IOS XE ソフトウェアに影響を与えます。該当するソフトウェアリリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

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。

改訂履歴

Version	Description	Section	Status	日付
1.1	Cisco バグ ID のリストを訂正しました。		Final	2017-September-07
1.0	Initial public release.		Final	2017-September-06

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。