

Cisco Nexus 9000シリーズスイッチの予約済みVLAN番号の脆弱性

Medium	アドバイザリーID : Cisco-SA-20150916-CVE-2015-6295	CVE-2015-6295
	初公開日 : 2015-09-16 16:08	
	バージョン 1.0 : Final	
	CVSSスコア : 4.8	
	回避策 : No Workarounds available	
	Cisco バグ ID :	

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 Nexus 9000シリーズスイッチ(N9K)の予約済みVLAN番号がタグ付けされた着信レイヤ2パケットの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、CPU使用率の上昇とコントロールプレーンの不安定性を原因とする部分的なサービス妨害(DoS)状態を引き起こす可能性があります。さらに、スイッチによって廃棄される必要があるレイヤ2パケットが、接続されたインターフェイスに誤って転送される可能性があります。

この脆弱性は、レイヤ2パケット内のVLAN番号の検証が行われないことに起因します。攻撃者は、N9Kの予約済みVLAN番号がタグ付けされた巧妙に細工されたレイヤ2パケットを送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はCPU使用率の上昇とコントロールプレーンの不安定性を原因とする部分的なDoS状態を引き起こす可能性があります。また、このパケットはN9Kによって廃棄される必要がありますが、接続されたネットワークに転送される可能性があります。

シスコはこの脆弱性を確認していますが、アップデートは提供されていません。

この脆弱性を不正利用するには、認証されていない攻撃者がローカルネットワークにアクセスする必要があります。この制限により、悪用される可能性が低くなります。

該当製品

シスコは登録ユーザ向けにBug ID [CSCuw13560](#)をリリースしました。このBug IDには追加の詳細情報と、影響を受ける製品バージョンの最新リストが含まれています。

脆弱性のある製品

このアラートが最初に公開された時点では、Cisco Nexus 9000シリーズソフトウェアリリース 6.1(2)I3(4)および7.0(3)I1(1)には脆弱性が存在していました。それ以降のリリースも影響を受ける可能性があります。

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。

回避策

今後のアップデートやリリースについては、ベンダーに連絡することを推奨します。

影響を受けるシステムを監視することを推奨します。

予約されているVLANの範囲を変更して、着信トラフィックと競合しないようにすることをお勧めします。

修正済みソフトウェア

更新プログラムは利用できません。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) 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を確認していません。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20150916-CVE-2015-6295>

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	初版リリース	適用外	Final	2015年9月16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。

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。