

Cisco NX-OS システム ソフトウェア ゲスト シェル 不正 な 内部 インターフェース アクセスの脆弱性

Medium	アドバイザーID : cisco-sa-20171129-nxos10	CVE-2017-12351
	初公開日 : 2017-11-29 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 5.7	
	回避策 : No workarounds available	
	Cisco バグ ID : CSCvf33038	

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 NX-OS システム ソフトウェアのゲスト シェル 機能の脆弱性はゲスト シェル コンテナの範囲外でパケットを読み、送信する認証された、ローカル攻撃者を可能にする可能性があります。攻撃者は有効な管理者の資格情報がこの攻撃を行うことを必要とします。

脆弱性はゲスト シェル 機能の不十分な内部 保全安全対策が原因です。攻撃者はゲスト シェル コンテナの外のデバイス内部 ネットワークのパケットを送信するか、または受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。

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-20171129-nxos10>

該当製品

脆弱性のある製品

この脆弱性は Cisco NX-OS システム ソフトウェアを実行する以下の製品に影響を及ぼします:

- Nexus 3000 シリーズ スイッチ
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ
- Nexus 9500 R シリーズ ラインカードおよびファブリック モジュール

該当する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。

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。

- Firepower 2100 シリーズ
- Firepower 4100 シリーズ次世代ファイアウォール
- Firepower 9300 セキュリティ アプライアンス
- マルチレイヤ ディレクタ スイッチ
- Nexus 1000V シリーズ スイッチ
- Nexus 2000 シリーズ ファブリック エクステンダ
- Nexus 3500 プラットフォーム スイッチ
- Nexus 5000 シリーズ スイッチ
- Nexus 5500 プラットフォーム スイッチ
- Nexus 5600 プラットフォーム スイッチ
- Nexus 6000 シリーズ スイッチ
- Nexus 7000 シリーズ スイッチ
- Nexus 7700 シリーズ スイッチ
- シスコ アプリケーション セントリック インフラストラクチャ (ACI) モードの Nexus 9000 シリーズ ファブリックスイッチ
- Unified Computing System マネージャ

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

修正済み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。

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。

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-20171129-nxos10>

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース	—	Final	2017-November-29

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。