# Cisco IOS 向け IOx ソフトウェアのゲスト オペレーティング システムで確認された不正アクセスの脆弱性


アドバイザリーID : cisco-sa-20190925-ios-gos-auth
CVE-2019-12648
初公開日 : 2019-09-25 16:00
バージョン 1.0 : Final
CVSSスコア : 9.9
回避策 : No workarounds available
Cisco バグ ID : CSCvm86480

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 ソフトウェア向けの IOx アプリケーション環境で脆弱性が確認されました。認証されたリモートの攻撃者が、標的デバイスで稼働中のゲスト オペレーティング システム（ゲスト OS）に不正アクセスする危険性があります。

この脆弱性は、権限の低いユーザが、管理者アカウントのみに制限する必要があるゲスト OS に対してアクセスを要求したときに、ロールベース アクセス制御（RBAC）が正しく評価されないことに起因します。権限の低いユーザのクレデンシャルを使用してゲスト OS 認証を行うことで、エクスプロイトされる可能性があります。エクスプロイトにより、攻撃者は root ユーザとしてゲスト OS へ不正アクセスできるようになります。

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。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-ios-gos-auth

このアドバイザリは、2019 年 9 月 25 日に公開された Cisco IOS および IOS XE ソフトウェア リリースのセキュリティ アドバイザリ資料の一部です。この資料には、13 件の脆弱性に関する 12 件のシスコ セキュリティ アドバイザリが記載されています。アドバイザリとリンクの一覧については、『Cisco Event Response: September 2019 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication』を参照してください。

# 該当製品

## 脆弱性のある製品

この脆弱性の影響を受けるのは、Cisco 800 シリーズ産業用サービス統合型ルータおよび Cisco 1000 シリーズ Connected Grid ルータ（CGR 1000）で、ゲスト OS を搭載した脆弱性のある Cisco IOS ソフトウェア リリースを稼動している場合です。

脆弱性が存在する Cisco IOS XE ソフトウェア リリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

ゲスト OS が有効になっているかどうかの確認

管理者は、デバイスの CLI で show iox host list detail コマンドを実行すると、ゲスト OS がデバイスで有効になっているかどうかを確認できます。

以下は、ゲスト OS が有効になっているデバイスで、このコマンドを実行した場合の出力例です。

<#root>

```
Router#
show iox host list detail | include OS status
```

<#root>

```
 OS status:
RUNNING
```

このコマンドが存在しない場合、または出力の OS ステータス フィールドに「RUNNING」の文字列が表示されない場合、そのデバイスはこのアドバイザリで説明されている脆弱性の影響を受けません。

## 脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が Cisco IOS XE ソフトウェア、Cisco IOS XR ソフトウェア、Cisco NX-OS ソフトウェアには影響を与えないことを確認しました。

# 詳細

シスコの産業用サービス統合型ルータおよび Cisco 1000 シリーズ Connected Grid ルータ（CGR 1000）デバイスは、ハイパーバイザ アーキテクチャ上に設計されています。このアーキテクチャでは、IOS とゲスト OS（Linux オペレーティングシステムなど）が 2 つの個別の仮想マシン（VM）として稼動します。

ゲスト OS は、ハイパーバイザ、IOS、およびゲスト OS イメージから構成されるバンドル IOS イメージの一部として使用できます。初回インストールまたはソフトウェア アップグレード用に Cisco IOS ソフトウェア イメージ バンドルをご使用の場合、ゲスト OS はソフトウェア イメージ バンドルの一環として自動的にインストールされます。

ゲスト OS へのアクセスは IOS のロールベース アクセス コントロール（RBAC）に依存しており、IOS で特権レベル 15 のクレデンシャルを持つユーザのみにアクセスを制限する必要があります。この脆弱性がエクスプロイトされると、攻撃者は権限の低い IOS ユーザのクレデンシャルを使用して、ゲスト OS にログインできるようになります。

このアドバイザリに記載されている脆弱性は、ゲスト OS インスタンス内で局所化されます。エクスプロイトによって、攻撃者はどのような状況でも、標的デバイスで稼働中の IOS ソフトウェアに対する管理アクセス権を取得できます。このような理由から、共通脆弱性評価システム（CVSS）のスコアでは「クリティカル（Critical）」という定型的表現に相当しますが、この脆弱性はセキュリティへの影響（SIR）が「High（高）」であると考えられます。

# 回避策

この脆弱性に対処する回避策はありません。

ゲスト OS を無効にすると、この脆弱性に対する攻撃ベクトルが排除されるため、対象デバイスのアップグレードが可能になるまでの適切な対応策となる可能性があります。管理者は、グローバル コンフィギュレーション モードで guest os <ID> image uninstall コマンドを実行すると、ゲスト OS をアンインストールできます。以下は、ゲスト OS がアンインストールされているデバイスに対して show platform guest-os コマンドを実行した場合の出力例です。

```
<#root>

Router#

show platform guest-os


Guest OS status:
Installation: Unknown
State:

 STOPPED
```

# 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リリースしています。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、アクセスまたはその他の方法で使用した場合、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、[シスコのセキュリティアドバイザリおよびアラート（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 Cisco Service Contract 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 POS 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。

## Cisco IOS ソフトウェア

お客様が Cisco IOS ソフトウェアの脆弱性による侵害の可能性を判断できるよう、シスコでは Cisco IOS Software Checker ツールを提供しています。このツールにより、特定の Cisco IOS ソフトウェア リリースに該当するシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。また該当

する場合、そのリリースに関するすべてのアドバイザリの脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用して次のタスクを実行できます。

- ドロップダウン リストからリリース（複数可）を選択するか、分析対象となるローカル システムからファイルをアップロードして、検索を開始する
- show version コマンドの出力をツールで解析する
- カスタマイズした検索（過去に公開されたすべてのシスコ セキュリティ アドバイザリを検索対象に入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべてのアドバイザリを含めるなど）を作成する

リリースが、公開されたシスコセキュリティアドバイザリのいずれかに該当するかどうかを確認するには、Cisco.comのCisco IOS Software Checkerを使用するか、次のフィールドにCisco IOSソフトウェアリリース(たとえば、15.1(4)M2)を入力します。

Check

デフォルトでは、Cisco IOS ソフトウェアのチェックには、結果は、高セキュリティへの影響の評価 (サー) または重大な脆弱性にのみが含まれています。「中間」の SIR 脆弱性の結果を含めるには、Cisco.com の Cisco IOS ソフトウェア チェッカーを使用して、[Impact Rating] ドロップダウン リストの [中間（Medium）] チェックボックスをオンにします。

## 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。

## 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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-ios-gos-auth

## 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 | 初回公開リリース | — | Final | 2019 年 9 月 25 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。

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。