Cisco IOS XE 3Sプラットフォームシリーズルートシェルライセンスバイパスの脆弱性

Medium	**アドバイザリーID :** cisco-sa-20151130-iosxe3s **初公開日 :** 2015-11-30 00:00 **最終更新日 :** 2015-12-14 21:35 **バージョン 2.2 :** Final **CVSSスコア :** 6.8 **回避策 :** Yes **Cisco バグ ID :** CSCuv93130	CVE-2015-6383

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 XE 3Sプラットフォーム用のCisco IOS XEオペレーティングシステムにおける診断コマンドの1つに存在する脆弱性により、認証された特権を持つローカルの攻撃者が *ルート*シェルアクセスを制限される可能性があります。 *root*シェルは、Cisco Technical Assistance Center(TAC)エンジニアによる高度なトラブルシューティング用に提供され、ライセンスが必要です。

この脆弱性は、コマンドラインインターフェイス(CLI)で診断コマンドに対するパラメータが適切に検証されていないために発生します。攻撃者は、特権レベル15で該当デバイスに認証され、診断コマンドに巧妙に細工されたパラメータを提供することで、この脆弱性をエクスプロイトする可能性があります。この不正利用により、認証された特権を持つ攻撃者が、 *ルート*シェルアクセスに必要なライセンスをバイパスできる可能性があります。認証されたユーザが *ルート*シェルアクセスを取得すると、さらに侵害され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で確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151130-iosxe3s

該当製品

脆弱性のある製品

Cisco IOS XE 3Sソフトウェアリリースを実行している場合、次のシスコ製品に脆弱性が存在します。

- Ciscoアグリゲーションサービス(ASR)ルータ1001
- Ciscoアグリゲーションサービス(ASR)ルータ1001-X
- Ciscoアグリゲーションサービス(ASR)ルータ1002-X
- Cisco Cloud Services Routers(CSR)1000V
- Ciscoサービス統合型ルータ(ISR)4321
- Ciscoサービス統合型ルータ(ISR)4331
- Ciscoサービス統合型ルータ(ISR)4351
- Ciscoサービス統合型ルータ(ISR)4431
- Ciscoサービス統合型ルータ(ISR)4451

Cisco IOS XE 3Sソフトウェアのすべてのバージョンは、制限付きルートシェルにアクセスするためにライセンスが必要な場合に脆弱性が存在します。

ライセンスが必要かどうかを判断するには、 **show license機能を使用します | include internal_service**コマンドを使用します。 **show license**コマンドが存在しない場合、または空の出力が返される場合、Cisco IOS XE 3Sプラットフォームには脆弱性はありません。

次に、ライセンスが必要で、脆弱性が存在するCisco IOS XE 3Sプラットフォームの例を示します。

```
#show license feature | include internal_service
internal_service         yes                   no               no
no           no
```

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

診断コマンドは、CLIでTACACS+コマンド許可を使用してブロックできます。ブロックするコマンドのリストと実装の手順については、次のリンクを参照してください。

http://www.cisco.com/web/about/security/intelligence/ios-xe-integrity-assurance.html#_Toc392234313

修正済みソフトウェア

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt の Cisco

Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、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 TAC もしくは契約しているメンテナンス プロバイダーまで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）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-20151130-iosxe3s

改訂履歴

バージョン	説明	セクション	ステータス	日付
2.2	「脆弱性が存在する製品」を更新し、製品に脆弱性があるかどうかを確認する方法の例を追加しました。	脆弱性が存在する製品	Final	2015年12月14日
2.1	「概要」を更新。回避策を追加。	概要、回避策	Final	2015年12月3日
2.0	パブリケーションのタイトルとID名が変更されました。また、影響を受ける製品を明らかにしました。	該当製品	Final	2015年12月3日
1.0	初版リリース	-	Final	2015年11月30日

利用規約

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。