Cisco UCS 6400および6500シリーズファブリックインターコネクトのIntersightマネージドモードにおけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-ucsfi-imm-syn-p6kZTDQC
CVE-2024-20344
初公開日 : 2024-02-28 16:00
バージョン 1.0 : Final
CVSSスコア : 5.3
回避策 : No workarounds available
Cisco バグ ID : CSCwb71517

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

Intersightマネージドモード(IMM)のCisco UCS 6400および6500シリーズファブリックインターコネクト(FI)におけるシステムリソース管理の脆弱性により、認証されていないリモート攻撃者が該当デバイスのデバイスコンソールUIでサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、該当デバイスへのTCP接続のレート制限が不十分であることに起因します。攻撃者は、大量のTCPパケットをデバイスコンソールのUIに送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はデバイスコンソールのUIプロセスをクラッシュさせ、DoS状態を引き起こす可能性があります。完全な機能を復元するには、ファブリックインターコネクトを手動でリロードする必要があります。

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、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsfi-imm-syn-p6kZTDQC

該当製品

脆弱性のある製品

公開時点では、この脆弱性は、IMM内で管理パッケージの脆弱性のあるリリースを実行していたCisco UCS 6400および6500シリーズファブリックインターコネクトに影響を与えました。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

デバイス設定の確認

デバイスで実行されているCisco IMM管理パッケージのリリースを確認するには、次の例に示すように、デバイスのCLIでshow versionコマンドを使用します。

```
<#root>

6500-FI#

show version

Device Connector Version: 1.0.11-9999

Management Package Version

: 1.0.11-1970
```

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UCSMマネージドモードのCisco UCSファブリックインターコネクトには影響を与えないことを確認しました。

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

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 セキュリティ アドバイザリ 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アップグレード ソリューション一式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。

修正済みリリース

Software-as-a-Service(SaaS)バージョンのIntersightを使用しているお客様は、要求されたデバイスで管理パッケージが自動的に更新されるため、ユーザ操作は必要ありません。Cisco Intersight仮想アプライアンスを使用しているお客様の場合、管理パッケージは仮想アプライアンスの更新後に更新されます。

発行時点では、次の表に示すリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左側の列にはシスコソフトウェアリリース、右側の列にはリリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースが示されています。

Cisco IMM管理パッケージリリース	First Fixed Release（修正された最初のリリース）
1.0.11 以前	1.0.11-1582
1.0.11-1583	脆弱性なし

注：デバイスで実行されているCisco IMM管理パッケージのリリースを確認するには、デバイスのCLIでshow versionコマンドを使用します。

Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、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は確認しておりません。

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-ucsfi-imm-syn-p6kZTDQC

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	2024年2月28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。