Cisco UCS Bシリーズ、マネージドCシリーズ、およびXシリーズサーバのRedfish APIにおけるコマンドインジェクションの脆弱性

Medium

アドバイザリーID : cisco-sa-cimc-redfish-cominj-sbkv5ZZ　CVE-2024-20365
初公開日 : 2024-10-02 16:00
バージョン 1.0 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwj57330

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 UCS Bシリーズ、Cisco UCS管理対象Cシリーズ、およびCisco UCS Xシリーズサーバの Redfish APIにおける脆弱性により、管理者権限を持つ認証されたリモートの攻撃者が、該当システムでコマンドインジェクション攻撃を実行し、権限をrootに昇格させる可能性があります。

この脆弱性は、不十分な入力検証に起因します。管理者権限を持つ攻撃者が、該当デバイスの Redfish APIを介して巧妙に細工されたコマンドを送信することにより、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 root に特権昇格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-cimc-redfish-cominj-sbkv5ZZ

該当製品

脆弱性のある製品

この脆弱性の公開時点では、次のシスコ製品に影響を与えていました。

- UCS B シリーズ ブレード サーバ

- UCSマネージドCシリーズラックサーバ
- UCS X シリーズ モジュラーシステム

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。

注： Redfishは、Cisco UCS Bシリーズ、Cisco UCS Managed Cシリーズ、およびCisco UCS Xシリーズサーバではデフォルトで有効になっています。アクセスするには、デバイスに管理IPアドレスを設定します。

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、この脆弱性がスタンドアロンモードのCisco UCS Cシリーズラックサーバ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

発行時点では、次の表に記載されている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。

UCS ManagerモードのUCS Bシリーズ、Cシリーズ、およびXシリーズサーバ

Cisco UCSサーバソフトウェア	First Fixed Release（修正された最初のリリース）
4.3 より前	脆弱性なし
4.3	4.3(4a)（その他すべてのプラットフォーム）

Cisco UCSサーバソフトウェア	First Fixed Release（修正された最初のリリース）
	4.3(4d)（UCS CシリーズM5）

Intersight ManagementモードのUCS Bシリーズサーバ

Cisco Intersightサーバファームウェアリリース	First Fixed Release（修正された最初のリリース）
4.2 より前	修正済みリリースに移行。
4.2	4.2(3j)
5.1	修正済みリリースに移行。
5.2	5.2（2.240051）

Intersight ManagementモードのUCS Cシリーズサーバ

Cisco Intersightサーバファームウェアリリース	First Fixed Release（修正された最初のリリース）
4.2 より前	修正済みリリースに移行。
4.2	4.2(3m)
4.3	4.3(4.240152)(M6、M7) 4.3(2.240090) (M5)

Intersight ManagementモードのUCS Xシリーズサーバ

Cisco Intersightサーバファームウェアリリース	First Fixed Release（修正された最初のリリース）
5.0	5.0(4g)
5.1	修正済みリリースに移行。
5.2	5.2（2.240053）

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-cimc-redfish-cominj-sbkv5ZZ

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10月2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。