Cisco NX-OSソフトウェアのCLI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-nxos-cmd-injection-xD9OhyOP
CVE-2024-20399
初公開日 : 2024-07-01 16:00
最終更新日 : 2024-07-03 18:36
バージョン 1.2 : Final
CVSSスコア : 6.0
回避策 : No workarounds available
Cisco バグ ID : CSCwj94682 CSCwj97011 CSCwj97007 CSCwj97009

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ソフトウェアのCLIにおける脆弱性により、管理者クレデンシャルを保有する認証されたユーザが、該当デバイスの基盤となるオペレーティングシステムでルートとして任意のコマンドを実行できるようになります。

この脆弱性は、特定の設定CLIコマンドに渡される引数の検証が不十分であることに起因します。攻撃者は、巧妙に細工された入力を該当の設定CLIコマンドの引数として含めることにより、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権限を使用して基盤となるオペレーティングシステムで任意のコマンドを実行できる可能性があります。

注：Cisco NX-OSデバイスでこの脆弱性の不正利用に成功するには、攻撃者が管理者クレデンシャルを持っている必要があります。次のシスコデバイスでは、すでにbash-shell機能を介して基盤となるオペレーティングシステムへのアクセスが管理者ユーザに許可されています。したがって、これらのデバイスでは、この脆弱性によって追加の特権が付与されることはありません。

- Nexus 3000 シリーズ スイッチ
- Cisco NX-OSソフトウェアリリース8.1(1)以降を実行しているNexus 7000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

シスコは特定のCisco NX-OSハードウェアプラットフォーム向けにソフトウェアアップデートをリリースしており、利用可能になった修正は引き続きリリースする予定です。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-nxos-cmd-injection-xD9OhyOP

該当製品

脆弱性のある製品

公開時点では、この脆弱性は、Cisco NX-OSソフトウェアの脆弱性のあるリリースを実行する次のシスコ製品に影響を与えました。

- MDS 9000シリーズマルチレイヤスイッチ(CSCwj97007)
- Nexus 3000シリーズスイッチ(CSCwj97009)[1]
- Nexus 5500プラットフォームスイッチ(CSCwj97011)
- Nexus 5600プラットフォームスイッチ(CSCwj97011)
- Nexus 6000シリーズスイッチ(CSCwj97011)
- Nexus 7000シリーズスイッチ(CSCwj94682)[2]
- スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ(CSCwj97009)[1]

1. Cisco Nexus 3000シリーズスイッチおよびCisco Nexus 9000シリーズスイッチをスタンドアロンNX-OSモードで実行しているCisco NX-OSソフトウェアリリースでは、bash-shell機能が使用できるため、この脆弱性によって追加の権限が付与されることはありません。Cisco NX-OSソフトウェアリリース9.3(5)以降は、次のシスコプラットフォームを除いて、この脆弱性の影響を受けません。

- Nexus 3000プラットフォーム：
  - N3K-C3264C-E
  - N3K-C3172PQ-10GE
  - N3K-C3172PQ-10GE-XL
  - N3K-C3172TQ-10GT
  - N3K-C3548P-10GX
- Nexus 9000プラットフォーム：
  - N9K-C92348GC-X(Cisco NX-OSソフトウェアリリース10.4(3)以降で修正)

2. Cisco Nexus 7000シリーズスイッチで実行されているCisco NX-OSソフトウェアリリース8.1(1)以降では、bash-shell機能が使用可能であるため、この脆弱性によって追加の権限が付与されることはありません。

この脆弱性の詳細については、このアドバイザリの「詳細情報」のセクションを参照してください。

脆弱性のある Cisco ソフトウェアリリースの詳細については、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。

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。

- 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- Firepower 1000 シリーズ
- Firepower 2100 シリーズ
- Firepower 4100 シリーズ
- Firepower 9300 セキュリティ アプライアンス
- Firepower Threat Defense（FTD）ソフトウェア
- VMware vSphere 向け Nexus 1000 Virtual Edge
- Nexus 1000V Switch for VMware vSphere
- ACI モードの Nexus 9000 シリーズ ファブリック スイッチ
- Cisco Secure Firewall 3100 シリーズ
- Cisco Secure Firewall 4200 シリーズ
- Secure Firewall Management Center(FMC)ソフトウェア
- UCS 6200 シリーズ ファブリック インターコネクト
- UCS 6300 シリーズ ファブリック インターコネクト
- UCS 6400 シリーズ ファブリック インターコネクト
- UCS 6500 シリーズ ファブリック インターコネクト

詳細

この脆弱性をエクスプロイトするには、攻撃者は管理者権限を持ち、特定のコンフィギュレーションコマンドにアクセスできる必要があります。

bash-shell機能をサポートしていないCisco NX-OSソフトウェアリリースをデバイスが実行している場合、Administrator権限を持つユーザがこの脆弱性を不正利用し、基盤となるオペレーティングシステムで任意のコマンドを実行する可能性があります。

デバイスで、bash-shell機能をサポートするCisco NX-OSソフトウェアリリースが実行されている場合、Administrator権限を持つユーザは、bash-shell機能を使用して基盤となるオペレーティングシステムにすでに直接アクセスできます。したがって、この脆弱性はデバイスに対する追加の権限を付与しません。ただし、この脆弱性を悪用すると、Administrator権限を持つユーザは、bash-shell機能を有効にせずに、またユーザがrun bash CLIコマンドを実行したことを示すシステムsyslogメッセージをトリガーせずに、基盤となるオペレーティングシステムでコマンドを実行できます。これは、管理者権限を持つユーザがデバイスのシェルコマンドの実行を非表示にするのに役立ちます。ただし、影響を受けるCLIコマンドは設定コマンドであるため、この脆弱性を不正利用するための最初のステップとして、設定変更がデバイスに適用されたことを報告するsyslogメッセージが表示されます。

bash-shell機能は、次のシスコデバイスでサポートされているすべてのCisco NX-OSソフトウェアリリースで使用できます。

- Nexus 3000 シリーズ スイッチ
- Cisco NX-OSソフトウェアリリース8.1(1)以降を実行しているNexus 7000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

標準的なネットワークプラクティスとして、管理ユーザnetwork-adminおよびvdc-adminのクレデンシャルを頻繁に監視し、変更する必要があります。また、予期しない設定変更がないかデバイスを監視する必要もあります。

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。

Cisco NX-OS ソフトウェア

お客様が Cisco NX-OS 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に、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべて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。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. 該当するソフトウェアを選択します。
3. 該当するプラットフォームを選択します。

4. リリース番号を入力します。たとえば、Cisco Nexus 3000 シリーズ スイッチの場合は 7.0(3)I7(5)、ACI モードの Cisco NX-OS ソフトウェアの場合は 14.0(1h) です。
5. [チェック (Check)] をクリックします。

2		Critical,High,Medium
このアドバイザのみ	Cisco NX-OS ソフトウェア	
あらゆるプラットフォーム		
Enter release number	オン	

関連情報

Cisco Nexus スイッチに最適な Cisco NX-OS ソフトウェアリリースの決定に際してサポートが必要な場合は、以下の推奨リリースに関するドキュメントを参照してください。セキュリティ アドバイザリでより新しいリリースが推奨されている場合は、そのアドバイザリのガイダンスに従うことをお勧めします。

Cisco MDS シリーズ スイッチ
VMware 向け Cisco Nexus 1000V スイッチ
Cisco Nexus 3000 Series Switches
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 5600 プラットフォームスイッチ
Cisco Nexus 6000 Series Switches
Cisco Nexus 7000 Series Switches
Cisco Nexus 9000 Series Switches
ACI モードの Cisco Nexus 9000 シリーズ スイッチ

Cisco UCS ソフトウェアに最適なリリースを確認するには、デバイスのリリースノートに記載されている推奨リリースに関するドキュメントを参照してください。

不正利用事例と公式発表

2024年4月、Cisco Product Security Incident Response Team(PSIRT)は、この脆弱性の不正利用が試みられたことを認識しました。

出典

シスコは、この脆弱性を報告していただいたSygnia社に感謝いたします。Cisco Advanced Security Initiatives Group(ASIG)のTristan Van Egroo氏がこの脆弱性を調査しました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.2	不正利用が発生する可能性のある条件を明確化し、脆弱性のない製品を追加。	概要、脆弱性が存在する製品、脆弱性を含んでいないことが確認された製品、詳細	Final	2024年7月3日
1.1	一部の製品については修正が提供され、その他の製品は提供が開始された時点でリリースされる予定であることを説明するために更新。	要約	Final	2024年7月2日
1.0	初回公開リリース	—	Final	2024年7月1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。