Cisco NX-OSソフトウェアのBashにおける任意のコード実行および権限昇格の脆弱性

Medium

アドバイザリーID : cisco-sa-nxos-bshacepe-bApeHSx7
初公開日 : 2024-08-28 16:00
バージョン 1.0 : Final
CVSSスコア : 6.7
回避策 : No workarounds available
Cisco バグ ID : CSCwh77783 CSCwh77791

CVE-2024-20411
CVE-2024-20413

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ソフトウェアの複数の脆弱性により、Bashシェルにアクセスする権限を持つ認証されたローカル攻撃者が、root権限で任意のコードを実行したり、該当デバイスでnetwork-admin権限に昇格したりする可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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。これら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-bshacepe-bApeHSx7

このアドバイザリは、2024年8月に公開されたCisco FXOSおよびNX-OSソフトウェアセキュリティアドバイザリバンドルの一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: August 2024 Semiannual Cisco FXOS and NX-OS 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

公開時点で、これらの脆弱性は、Cisco NX-OSソフトウェアの脆弱性が存在するリリースを実行していて、Bashシェルが有効になっているか、ログイン時にBashシェルを使用するように

設定されたユーザである次のシスコ製品に影響を与えました。

- Nexus 3000 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

脆弱性が存在する Cisco 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。

Bashシェルが有効になっているかどうかの確認

Bashシェルが有効になっているかどうかを確認するには、show feature | include bash CLIコマンドを使用します。次に例を示します。

<#root>

```
switch# show feature | include bash
bash-shell             1          enabled
```

注：この機能はデフォルトでは無効になっています。

ログイン時にBashシェルを使用するようにユーザが設定されているかどうかを確認する

ユーザがログイン時にBashシェルを使用するように設定されているかどうかを確認するには、show running-config | include shelltype CLIコマンドを使用します。次に例を示します。

<#root>

```
switch# show running-config | include shelltype
username testuser shelltype bash
```

結果が返されない場合、ログイン時のBashシェルは設定されていません。

注：shelltype bashを使用するように設定されているユーザは、ログインに成功するとBashシェルを使用するようになります。この場合、Bashシェルを有効にする必要はありません。

Bashシェルの許可は、network-adminまたはdev-opsロールを持つユーザ、カスタムのロールベースアクセスコントロール(RBAC)ロールを持つユーザ、またはshelltype bashが設定されているユーザに制限されていました。これらの脆弱性に対する修正に加えて、network-adminロールまたはカスタムRBACロールを持つユーザだけにBashシェルのアクセスを制限し、bashコマンドの実行を明示的に許可する強化策が追加されています。詳細については、次のバグIDを

参照してください。

- CSCwj42387:dev-opsロールのBashシェルアクセスの削除
- CSCwj51942:Bashシェルのアクセスをnetwork-adminロールだけに制限する

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、これら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、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- 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
- MDS 9000 シリーズ マルチレイヤ スイッチ
- VMware vSphere 向け Nexus 1000 Virtual Edge
- Nexus 1000V Switch for VMware vSphere
- Nexus 5500 プラットフォーム スイッチ
- Nexus 5600 プラットフォーム スイッチ
- Nexus 6000 シリーズ スイッチ
- Nexus 7000 シリーズ スイッチ
- 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
- 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

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために、他の脆弱性をエクスプロイトする必要はありません。また、いずれかの脆弱性の影響を受けるリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2024-20411:Cisco NX-OSソフトウェアにおける任意のコード実行の脆弱性

Cisco NX-OSソフトウェアの脆弱性により、Bashシェルにアクセスする権限を持つ認証された口

ーカル攻撃者が、該当デバイスでルートとして任意のコードを実行できるようになります。

この脆弱性は、Bashシェルからコマンドを実行する際のセキュリティ制限が不十分であることに起因します。Bashシェルにアクセスする権限を持つ攻撃者は、基盤となるオペレーティングシステムで特定の巧妙に細工されたコマンドを実行することにより、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権限で任意のコードを実行でき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。

バグID:CSCwh77791
CVE ID：CVE-2024-20411
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.7
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVE-2024-20413:Cisco NX-OSソフトウェアの権限昇格の脆弱性

Cisco NX-OSソフトウェアの脆弱性により、Bashシェルにアクセスする権限を持つ認証された口ーカル攻撃者は、該当デバイスで権限をnetwork-adminに昇格させることができます。

この脆弱性は、Bashシェルからアプリケーション引数を実行する際のセキュリティ制限が不十分であることに起因します。Bashシェルにアクセスする権限を持つ攻撃者は、基盤となるオペレーティングシステムで巧妙に細工されたコマンドを実行することにより、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network-adminの権限を使用して新しいユーザを作成できます。

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。

バグID:CSCwh77783
CVE ID：CVE-2024-20413
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.7
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

回避策

これら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 | Check

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

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例とその公表は確認しておりません。

出典

この脆弱性は、シスコ内部でのシステム 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-nxos-bshacepe-bApeHSx7

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8月28日

利用規約

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。