Cisco NX-OS ソフトウェアの Call Home コマンドインジェクションに関する脆弱性

アドバイザリーID : cisco-sa-callhome-cmdinj-zkxzSCY
初公開日 : 2020-08-26 16:00
最終更新日 : 2020-08-26 20:51
バージョン 1.1 : Final
CVSSスコア : 7.2
回避策 : No workarounds available
Cisco バグ ID : CSCve15011 CSCvg11732 CSCvg11752 CSCvg11715 CSCvh85161

CVE-2020-3454

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 Call Home 機能に存在する脆弱性により、認証されたリモートの攻撃者が、基盤となるオペレーティングシステムで root 権限を使用して実行可能な任意のコマンドを注入する可能性があります。

この脆弱性は、Cisco NX-OS ソフトウェアでトランスポート方式がHTTP に設定されている場合に、特定の Call Home 設定パラメータの入力検証が不十分であることに起因します。攻撃者は、該当デバイスの Call Home 設定でパラメータを変更することで、この脆弱性をエクスプロイトできます。エクスプロイトに成功すると、基盤となる OS でルート権限を使用して任意のコマンドを実行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-callhome-cmdinj-zkxzSCY

このアドバイザリは 2020 年 8 月に公開された Cisco FXOS および NX-OS ソフトウェアのセキュリティ アドバイザリ バンドルの一部です。この中には、7 件の脆弱性に関する 7 件のシスコセキュリティ アドバイザリが含まれています。これらのアドバイザリとそのリンクの一覧については、『Cisco Event Response: August 2020 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

この脆弱性の影響を受けるのは、次のシスコ製品で 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おり、かつ Call Home 機能でトランスポート方式に HTTP が設定されている場合です。

- MDS 9000 シリーズ マルチレイヤスイッチ (CSCvh85161)
- Nexus 3000 シリーズ スイッチ (CSCvg11715)
- Nexus 3600 プラットフォーム スイッチ (CSCvg11752) [1]
- Nexus 5500 プラットフォームスイッチ (CSCve15011)
- Nexus 5600 プラットフォームスイッチ (CSCve15011)
- Nexus 6000 シリーズ スイッチ (CSCve15011)
- Nexus 7000 シリーズ スイッチ (CSCvg11732)
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ (CSCvg11715)
- Nexus 9500 R シリーズ スイッチング プラットフォーム (CSCvg11752) [1]

1.脆弱性は別のバグIDで修正されているため、このアドバイザリに限り、Cisco Nexus 3600プラットフォームスイッチとNexus 9500 Rシリーズスイッチングプラットフォームは、Cisco Nexus 3000および9000シリーズスイッチとは別に記載されています。

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。

Call Home 機能のトランスポート方式が HTTP に設定されているかどうかの確認

Call Home 機能でトランスポート方式が HTTP に設定されているかどうかを確認するには、show running-config callhome コマンドを実行して、次の要素が表示されるかを確認します。

```
callhome
  email-contact xxyy@zzz.com
  destination-profile full_txt transport-method http
  destination-profile full_txt http http://<snip>
  enable
```

宛先プロファイル URL は、HTTP または HTTPS を使用するように設定できます。HTTP と HTTPS の両方が影響を受けます。

Cisco Nexus 3000 および 9000 シリーズ スイッチでソフトウェアリリース 9.3(1) 以降を実行している場合、HTTP URL のコマンド構文には、index と number という 2 つの追加パラメータがあります。それ以外の設定は同じです。次の例は、デバイスで HTTPS を使用するように設定されている場合のコマンド構文を示しています。

```
destination-profile full_txt index 1 http https://<snip>
```

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。

- 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
- VMware vSphere 向け Nexus 1000 Virtual Edge
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 9000 シリーズ ファブリック スイッチ（アプリケーション セントリック インフラストラクチャ（ACI）モード）
- 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

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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は https://www.cisco.com/c/en/us/products/end-user-license-agreement.html に記載のシスコのソフトウェアライセンスの条項に従うことに同意したことになります。

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェ

ア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

Cisco NX-OS ソフトウェア

お客様が Cisco NX-OS 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、シスコでは Cisco Software Checker を提供しています。このツールにより、特定の Cisco NX-OS ソフトウェアリリースに該当するシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。また該当する場合、そのリリースに関するすべてのアドバイザリ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。

お客様は、Cisco Software Checker を使用して次の方法でアドバイザリを検索できます。

- ソフトウェア、プラットフォーム、および 1 つ以上のリリースを選択する
- 特定のリリースのリストを含む .txt ファイルをアップロードする
- show version コマンドの出力を入力する

検索を開始した後で、すべてのシスコ セキュリティ アドバイザリまたは 1 つ以上の特定のアドバイザリが含まれるように検索をカスタマイズできます。

また、次のフォームを使用して、Cisco NX-OS ソフトウェアとプラットフォームを選択、およびリリースを入力することで（例：Cisco Nexus 3000 シリーズ スイッチの 7.0(3)I7(5)、ACI モードの Cisco NX-OS ソフトウェアの 14.0(1h)）、シスコ セキュリティ アドバイザリの対象となるリリースであるかを判断することもできます。

Cisco NX-OS ソフトウェア	MDS 9000 シリーズ マルチレイヤ スイッチ

Enter Version	Check

デフォルトでは、Cisco Software Checker の結果には、Security Impact Rating（SIR）が「重大」または「高」の脆弱性だけが含まれます。「中間」の SIR 脆弱性の結果を含めるには、Cisco Software Checker を使用して、検索をカスタマイズするときに [影響の評価（Impact Rating）] ドロップダウンリストの [中間（Medium）] チェックボックスをオンにします。

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 スイッチ向け Cisco Nexus 1000V
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）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。

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-callhome-cmdinj-zkxzSCY

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	ソフトウェアチェッカーのリンクを修正。	修正済みソフトウェア	Final	2020 年 8 月 26 日
1.0	初回公開リリース		Final	2020 年 8 月 26 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。