アプリケーション セントリック インフラストラクチャ モードの Cisco Nexus 9000 シリーズ ファブリック スイッチにあるデフォルトの SSH キーの脆弱性

Critical

アドバイザリーID : cisco-sa-20190501-nexus9k-sshkey

CVE-2019-1804

初公開日 : 2019-05-01 16:00

最終更新日 : 2019-05-09 12:49

バージョン 1.2 : Final

CVSSスコア : 9.8

回避策 : No workarounds available

Cisco バグ ID : CSCvo80686

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

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) モードで動作する Cisco Nexus 9000 シリーズ スイッチ ソフトウェアの SSH キー管理の脆弱性により、認証されていないリモートの攻撃者が、*ルート ユーザ*の特権を使用して該当システムに接続できる危険性があります。

この脆弱性は、すべてのデバイスにあるデフォルトの SSH キー ペアの存在に起因します。 攻撃者は、抽出されたキー情報を使用して IPv6 でターゲット デバイスへの SSH 接続を開くことにより、この脆弱性を エクスプロイトする危険性があります。 この脆弱性により、攻撃者が*ルート ユーザ*の特権を使用してシステムにアクセスできる危険性があります。 この脆弱性は、IPv6 でのみエクスプロイトすることが可能です。 IPv4 には脆弱性はありません。

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ました。 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-nexus9k-sshkey

該当製品

脆弱性のある製品

この脆弱性は、13.2(6i) または 14.1(1i) より前の Cisco Nexus 9000 シリーズ ACI モード スイッチ ソフトウェア リリースを実行している場合に、次のシスコ製品に影響を与えます。

- 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）

Cisco NX-OS ソフトウェア リリースの判別

管理者は、デバイスの CLI で show version コマンドを使用して、デバイスで実行されている Cisco NX-OS ソフトウェアのリリースを確認できます。 次の例は **11.2(2)** リリースを示しています。

```
nxos-n9k-aci# show version
Cisco Nexus Operating System (NX-OS) Software
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and http://www.opensource.org/licenses/lgpl-
2.1.php
Software
BIOS:      version N/A
kickstart: version 11.2(2) [build 11.2(1.184)]
system:    version 11.2(2) [build 11.2(1.184)]
...
```

Application Policy Infrastructure Controller ソフトウェア リリースの確認

Application Policy Infrastructure Controller（APIC）のソフトウェアと、ACI モードの Cisco Nexus 9000 シリーズ ファブリック スイッチは、1 対 1 でマッピングされています。 デバイスで実行されている Cisco APIC ソフトウェア リリースを確認する際には、Cisco NX-OS ソフトウェア バージョン番号の左端の数字は無視してください。 上記の例の出力には、Cisco APIC ソフトウェア リリース 1.2(2) にマッピングされた、Cisco NX-OS ソフトウェア **バージョン 11.2(2)** が示されています。

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が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

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 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
- Nexus 1000V Switch for Microsoft Hyper-V

- Nexus 1000V Switch for VMware vSphere
- Nexus 3000 シリーズ スイッチ
- Nexus 3500 プラットフォーム スイッチ
- Nexus 3600 プラットフォーム スイッチ
- 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
- Nexus 7700 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
- Nexus 9500 R シリーズ スイッチング プラットフォーム
- 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 アップデートを提供しています。 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載された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。 https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

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、Cisco Security Advisories and Alerts 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完全なアップグレード ソリューション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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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 に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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。

修正済みリリース

この脆弱性は、ACI モードの Cisco Nexus 9000 シリーズ スイッチ ソフトウェア リリース 13.2(6i)、14.1(1i)、以降で修正されています。

関連情報

Cisco Nexus スイッチに最適な Cisco NX-OS ソフトウェア リリースの決定に関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 シリーズおよび 3500 シリーズ スイッチ
Cisco Nexus 5000 シリーズ スイッチ
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 6000 Series Switches
Cisco Nexus 7000 シリーズ スイッチ
Cisco Nexus 9000 シリーズ スイッチ
ACI モードの Cisco Nexus 9000 シリーズ スイッチ

Cisco UCS に最適な Cisco NX-OS ソフトウェア リリースの確認に関してサポートが必要な場合は、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やその公表を確認していません。

出典

ERNW Research 社と協力関係にある ERNW Enno Rey Netzwerke 社の Oliver Matula 氏に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-nexus9k-sshkey

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.2	ソフトウェア リリース 13.2(6i) が修正済みとして追加されました。	「脆弱性のある製品」および「修正済みソフトウェア」	最終版	2019年5月9日
1.1	製品名をより具体的なものに変更。	脆弱性のある製品	Interim	2019年5月2日
1.0	初回公開リリース		Interim	2019年5月1日

利用規約