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 スイッチにおける特権昇格の脆弱性

High

アドバイザリーID : cisco-sa-20190501-aci-hw-clock-util
CVE-2019-1592
初公開日 : 2019-05-01 16:00
最終更新日 : 2019-05-09 15:55
バージョン 1.1 : Final
CVSSスコア : 7.8
回避策 : No workarounds available
Cisco バグ ID : CSCvm64104

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 ソフトウェアのバックグラウンド処理機能の脆弱性により、認証されたローカルの攻撃者が該当デバイスでルートとして昇格された特権を取得できる可能性があります。

この脆弱性は、該当デバイスでユーザが指定したファイルの検証が十分に行われないことに起因します。攻撃者が該当デバイスの CLI にログインし、ファイルシステムの特定のディレクトリで細工したファイルを作成することにより、この脆弱性をエクスプロイトする可能性があります。エクスプロイトが成功すると、攻撃者は該当デバイスでルートとして任意のオペレーティング システム コマンドを実行できる危険性があります。

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。

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-20190501-aci-hw-clock-util

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。該当するソフトウェア 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」の項を参照してください。

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。

```
<#root>

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)]

.
.
.
```

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 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 2000 シリーズ ファブリック エクステンダ
- 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 5000 シリーズ 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 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、[シスコのセキュリティアドバイザリおよびアラート（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 Cisco Service Contract 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 POS 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。

該当バージョンのデバイスを実行しているすべてのお客様には、最新のメンテナンス バージョンまたは最新の Long-Lived バージョンにアップグレードすることを推奨します。シスコでは、お客様がhttps://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/recommended-release/b_Recommended_Cisco_ACI_Releases.htmlページにアクセスして、どの修正済みリリースを選択するかを確認することを推奨します。

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 Series Switches
Cisco Nexus 5500 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 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）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

この脆弱性を報告していただいた Octav Opaschi 氏と Detack 社に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-aci-hw-clock-util

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	修正済みソフトウェアの情報を更新。	「脆弱性のある製品」および「修正済みリリース」	Final	2019 年 5 月 9 日
1.0	初回公開リリース	—	Final	2019 年 5 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。