

Cisco Enterprise NFV インフラストラクチャ ソフトウェアにおける任意ファイルの読み取り/書き込みの脆弱性



アドバイザーID : cisco-sa-20190703-[CVE-2019-1894](#)
nfvis-file-readwrite

初公開日 : 2019-07-03 16:00

バージョン 1.0 : Final

CVSSスコア : [7.2](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvn12407](#)

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 Enterprise NFV インフラストラクチャ ソフトウェア (NFVIS) の脆弱性により、管理者権限を持つ認証されたリモートの攻撃者が、該当デバイスの基盤となるオペレーティング システム (OS) 上の任意のファイルを上書きまたは読み取ることができるようになります。

この脆弱性は、NFVIS ファイル システム コマンドの不適切な入力検証に起因します。攻撃者は、該当コマンドの実行中に巧妙に細工された変数を使用して、この脆弱性をエクスプロイトする可能性があります。攻撃者は、エクスプロイトに成功すると、基盤となる OS 上の任意のファイルを上書きまたは読み取ることが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。

このアドバイザーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-nfvis-file-readwrite>

該当製品

脆弱性のある製品

この脆弱性は、3.10.1 以前の Cisco Enterprise NFV インフラストラクチャ ソフトウェア (NFVIS) リリースに影響を与えます。

Cisco Enterprise NFVIS リリースの判別

デバイスで実行している Cisco Enterprise NFVIS リリースは、管理者が CLI から show version コマンドを実行することで確認できます。次に、デバイスが Cisco Enterprise NFVIS リリース 3.11.2 を実行しているデバイスのこのコマンドの出力例を示します。

```
<#root>
nfvis#
show version

Cisco NFV Infrastructure Software
Version 3.11.2-FC2
.
.
.
```

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。](#)

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です。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

シスコは、Cisco Enterprise NFVIS リリース 3.10.1 以降でこの脆弱性を修正しました。

お客様は、次の手順で Cisco.com の [Software Center から Cisco Enterprise NFVIS をダウンロードできます。](#)

1. [すべてを参照 (Browse All)] をクリックします。
2. [Routers (ルータ)] > [Network Functions Virtualization (ネットワーク機能の仮想化)] > [Enterprise NFV Infrastructure Software (Enterprise NFV インフラストラクチャ ソフトウェア)] > [NFV Infrastructure Software (NFV インフラストラクチャ ソフトウェア)] の順に選びます。
3. Enterprise NFV インフラストラクチャ ソフトウェア ページの左側のペインを使用してリリースにアクセスします。

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

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	2019年7月3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、単独の転載や意識を施した場合、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。