Cisco NX-OS ソフトウェア パッチ署名の検証バイパスの脆弱性

Medium	**アドバイザリーID :** cisco-sa-20190515-nxos-psvb **初公開日 :** 2019-05-15 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.4 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvj12239 CSCvi42264	CVE-2019-1809

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 ソフトウェアのイメージ署名の検証機能の脆弱性は管理者レベル 資格情報が付いている影響を受けたデバイスで悪意のあるソフトウェアパッチをインストールする認証された、ローカル攻撃者を可能にする可能性があります。

脆弱性はパッチ イメージのためのデジタル署名の不適当な確認が原因です。 攻撃者は無署名のソフトウェアパッチを細工 し、影響を受けたデバイスでロードすることによってこの脆弱性をシグニチャ チェックをバイパスするために不正利用する可能性があります。 正常なエクスプロイトは攻撃者が悪意のあるソフトウェアパッチ イメージを起動することを可能にす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-20190515-nxos-psvb

該当製品

脆弱性のある製品

本脆弱性は、Cisco NX-OS ソフトウェアの脆弱性のあるリリースを実行する次のシスコ製品に影響を与えます。

- MDS 9700 シリーズ マルチレイヤ ディレクタ[1]
- Nexus 7000 シリーズ スイッチ
- Nexus 7700 シリーズ スイッチ
- 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

1. MDS 製品に関しては、MDS 9700 シリーズ マルチレイヤ ディレクタだけこの脆弱性から影響を受けます。 他の MDS 9000 シリーズ マルチレイヤ スイッチはすべて脆弱ではないです。

脆弱性が存在する Cisco NX-OS 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。

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（MDS 9700）[1] を除いて
- 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 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）
- 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 6400 シリーズ ファブリック インターコネクト

1. MDS 製品に関しては、MDS 9700 シリーズ マルチレイヤ ディレクタだけこの脆弱性から影響を受けます。 他の MDS 9000 シリーズ マルチレイヤ スイッチはすべて脆弱ではないです。

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

アップグレード アクションは行進 2019 Cisco FXOS をおよび NX-OS ソフトウェア 当たるために既に推奨されるリリースをバンドル加えてしまった顧客向けに必要ではないです。 Cisco イベント応答が表示されて下さい: 行進 2019 Cisco FXOS および NX-OS ソフトウェア Security

Advisory はバンドルのアドバイザリのリストのためのパブリケーションを組み込みました。

行進に 2019 のバンドルを当たるために推奨されるリリースを加えなかった顧客はこのセクションの適当な表に示すように適切なリリースにアップグレードするように勧告されます。 次の表では、左の列は Cisco NX-OS ソフトウェア リリースをリストします。 右の列はこの脆弱性のための修正を含む最初のリリースを示します。

MDS 9700 シリーズ マルチレイヤ ディレクタ: CSCvi42264

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース
5.2	脆弱性なし
6.2	脆弱性なし
7.3	8.1(1a)
8.1	8.1(1a)
8.2	8.3(1)
8.3	脆弱性なし

Nexus 7000 および 7700 シリーズ スイッチ CSCvi42264

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース
6.2 より前	脆弱性なし
6.2	脆弱性なし
7.2	7.3(3)D1(1)
7.3	7.3(3)D1(1)
8.0	8.2(3)
8.1	8.2(3)
8.2	8.2(3)
8.3	脆弱性なし

UCS 6200、6300 ファブリック インターコネクト： CSCvj12239

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース
3.1 より前	脆弱性なし
3.1	3.2(3k)
3.2	3.2(3k)
4.0	脆弱性なし

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

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-psvb

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019-May-15

利用規約

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。