Cisco IOS および IOS XE ソフトウェア情報公開脆弱性

Medium	**アドバイザリーID :** cisco-sa-20190327-info **初公開日 :** 2019-03-27 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 4.4 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvi66418 CSCvg97571	CVE-2019-1762

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 IOS および IOS XE ソフトウェアのセキュア ストレージ 機能の脆弱性は影響を受けたデバイスの敏感なシステム情報にアクセスする認証された、ローカル攻撃者を可能にする可能性があります。

脆弱性は影響を受けたソフトウェアが設定アップデートを処理するとき暗号化時に実行された不適当なメモリ オペレーションが原因です。 攻撃者は影響を受けたデバイスの特定の記憶域のコンテンツの取得によってこの脆弱性を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重要なシステム 情報を回復 するのに使用することができる、デバイスコンフィギュレーションの一部であるキーイングマテリアルの公開という結果に終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-20190327-info

該当製品

脆弱性のある製品

この脆弱性は Cisco IOS または IOS XE ソフトウェアの脆弱なリリースを実行している有効に

なるセキュア ストレージ 機能が付いている Ciscoデバイスに影響を与えます。

このアドバイザリにリンクされる 2 つのバグがありますその両方とも同じ脆弱性に対処する:

- Ciscoバグ CSCvg97571 は 15.6(3) M1 後続のリリースのコード変更を当たるために育てられました。
- Ciscoバグ CSCvi66418 は Cisco IOS XE ソフトウェア リリース 16.6.1 または後続のリリースのコード変更を当たるために育てられました。

脆弱性が存在する Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの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。

セキュア ストレージが有効に なるかどうか判別します

セキュア ストレージ 機能がデバイスで有効に なるかどうか判別する 2 つのメソッドがあります:

*オプション 1： **show running-config all** の使用 | **サービス private 構成暗号化** コマンドを**含んで下さい**。*

デバイスが有効に なるセキュア ストレージ 機能で設定されるかどうか判別するために **show running-config all** を使用して下さい | デバイスの**サービス private 構成暗号化** privileged exec コマンドを**含んで下さい**。 以下は、 **show running-config all** の出力例です。 | 有効に なるセキュア ストレージ 機能を備えている Ciscoデバイスの**サービス private 構成暗号化** コマンドを**含んで下さい**。

```
Router#show running-config all | include service private-config-encryption
service private-config-encryption
```

このコマンドが存在しない場合、またはその他の出力が生成される場合、デバイスはこのアドバイザリで説明されている脆弱性の影響を受けていません。

*オプション 2： **提示パーサー 暗号化 ファイル ステータス**の使用 | **機能** コマンドを**含んで下さい**。*

セキュア ストレージ 機能がデバイスで有効に なるかどうか判別するために、**提示パーサー 暗号化 ファイル ステータスを**使用して下さい | デバイスの**機能** privileged exec コマンドを**含んで下さい**。 次の例は**提示パーサー 暗号化 ファイル ステータス**の出力を示したものです | 有効に なるセキュア ストレージ 機能を備えている Ciscoデバイスの**機能** コマンドを**含んで下さい**。

```
Router#show parser encrypt file status | include Feature
Feature: Enabled
```

このコマンドが存在しない場合、またはその他の出力が生成される場合、デバイスはこのアドバイザリで説明されている脆弱性の影響を受けていません。

Cisco IOS ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS ソフトウェア リリースは、管理者がデバイスにログインして、CLI で **show version** コマンドを使用し、表示されるシステム バナーを参照することにより確認できます。 デバイスが Cisco IOS ソフトウェアを実行している場合、システム バナーに「*Cisco Internetwork Operating System Software*」や「*Cisco IOS Software*」などのテキストが表示されます。 バナーにはインストールされたイメージ名もカッコ内に表示され、その後ろに、Cisco IOS ソフトウェアのリリース番号とリリース名が表示されます。 一部のシスコ デバイスでは、**show version** コマンドをサポートしていなかったり、別の出力が表示されたりします。

次に、Cisco IOS ソフトウェア リリース 15.5(2)T1 が実行されていて、インストールされているイメージ名が *C2951-UNIVERSALK9-M* であるデバイスでのコマンド出力例を示します。

```
Router> show version

Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.5(2)T1, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Mon 22-Jun-15 09:32 by prod_rel_team
.
.
.
```

Cisco IOS ソフトウェア リリースの命名と番号付けの規則に関する詳細は、『Cisco IOS and NX-OS Software Reference Guide』を参照してください。

Cisco IOS XE ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS XE ソフトウェア リリースは、管理者がデバイスにログインして、CLI で **show version コマンド**を実行し、表示されるシステム バナーを参照することにより確認できます。 デバイスが Cisco IOS XE ソフトウェアを実行している場合、システム バナーに「*Cisco IOS Software*」、「*Cisco IOS XE Software*」などのテキストが表示されます。

次に、Cisco IOS XR ソフトウェア リリース 16.2.1 が実行されていて、インストールされているイメージ名が *CAT3K_CAA-UNIVERSALK9-M* であるデバイスでのコマンドの出力例を示します。

```
ios-xe-device# show version

Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali
16.2.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Sun 27-Mar-16 21:47 by mcpre
.
```

.
.

Cisco IOS XE ソフトウェア リリースの命名と番号付けの規則に関する詳細は、『Cisco IOS and NX-OS Software Reference Guide』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 Cisco IOS XR ソフトウェアまたは Cisco NX-OS ソフトウェアには影響を与えないことを確認しました。

詳細

Cisco IOS および IOS XE ソフトウェアはセキュア ストレージ 暗号形式でそれを保存することによって重要な構成情報を保護するために割り当て管理者を特色にします。 該当するソフトウェア リリースは暗号化されたバージョンとともにコンフィギュレーション ファイルの非暗号化バージョンのストレージという結果に終るかもしれない完全な暗号化 バッファ クリーンアップを行わないかもしれません。 攻撃者はデバイスコンフィギュレーションを保存するのに使用する記憶装置にマッピング される特定の記憶域のコンテンツの取得によってこの脆弱性を利用できます。

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

影響を受けたおよび修正済みソフトウェアリリースについての詳細な情報に関しては、Cisco IOSソフトウェア チェッカーを参照して下さい。

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。

Cisco IOS および IOS XE ソフトウェア

Cisco IOS ソフトウェアおよび IOS XE 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 IOS Software Checker ツールを提供しています。このツールにより、特定のソフトウェア 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。

このツールを使用して次のタスクを実行できます。

- ドロップダウン リストからリリース（複数可）を選択するか、分析対象となるローカル システムからファイルをアップロードして、検索を開始する
- **show version** コマンドの出力をツールで解析する
- カスタマイズした検索（過去に公開されたすべてのシスコ セキュリティ アドバイザリを検索対象に入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべてのアドバイザリを含めるなど）を作成する

リリースが、公開されたシスコ セキュリティ アドバイザリのいずれかに該当するかどうかを確認するには、Cisco.com の Cisco IOS Software Checker を使用するか、以下のフィールドに Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェア リリース（たとえば、**15.1(4)M2**、**3.13.8S** など）を入力します。

デフォルトでは、Cisco IOS ソフトウェアのチェックには、結果は、高セキュリティへの影響の評価 (サー) または重大な脆弱性にのみが含まれています。 「中間」の SIR 脆弱性の結果を含めるには、Cisco.com の Cisco IOS ソフトウェア チェッカーを使用して、[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。

Cisco IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについては、Cisco IOS XE ソフトウェアのリリースに応じて「Cisco IOS XE 2 Release Notes」、「Cisco IOS XE 3S Release Notes」、または「Cisco IOS XE 3SG Release Notes」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

この脆弱性は、Cisco TAC のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-info

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 年 3 月 27 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。