# Cisco 適応型セキュリティ アプライアンス ソフトウェアの Web ベースの管理インターフェイスにおける特権昇格の脆弱性

High

**アドバイザリーID :** cisco-sa-20190807-asa-privescala

**初公開日 :** 2019-08-07 16:00

**バージョン 1.0 :** Final

**CVSSスコア :** 8.8

**回避策 :** No workarounds available

**Cisco バグ ID :** CSCvp09150

CVE-2019-1934

**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 適応型セキュリティ アプライアンス ( ASA ) ソフトウェアの Web ベース管理インターフェイスで見つかった脆弱性により、認証済みのリモート攻撃者が、特権を昇格し、影響を受けるデバイスで管理機能を実行する可能性があります。

この脆弱性は、認証に対する不十分な検証に起因します。 攻撃者は、影響を受けるデバイスに権限の低いユーザとしてログインし、最初のログイン時に取得した情報を使用して管理機能を実行する特定の HTTPS 要求を送信することで、この脆弱性を不正利用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-20190807-asa-privescala

## 該当製品

### 脆弱性のある製品

この脆弱性は、Cisco ASA ソフトウェア リリース 8.2 以降を実行中で、Web 管理アクセスが有効になっているシスコ製品に影響を及ぼします。

### Web 管理アクセスが設定されているかどうかの確認

管理者は、**show running-config http** コマンドを使用して Web 管理が有効になっているかどうかを確認できます。 次の例は、Web 管理機能が有効になっており、10.10.10.0/24 ネットワークから「Management」（管理）インターフェイスを介して Web 管理機能にアクセスできるデバイスに関するコマンドの出力を示しています。

```
ciscoasa# show running-config http

http server enable
http 10.10.10.0 255.255.255.0 Management
```

**注:** デバイスは、**http <remote_ip_address> <remote_subnet_mask> <interface_name>** コマンドで設定された範囲内の IP アドレスから送信された要求についてのみ、脆弱性を持ちます。

### 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 Cisco Firepower Threat Defense（FTD）ソフトウェアに影響を及ぼさないことを確認しました。

## 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**

次の表に示すように、該当する修正済みのソフトウェア リリースにアップグレードすることをお勧めします。

| Cisco ASA ソフトウェア リリース | First Fixed Release（修正された最初のリリース） |
|---|---|
| 先により 9.4[1] | 9.4.4.37 |
| 9.4 | 9.4.4.37 |
| 9.5[1] | 9.6.4.30 |
| 9.6 | 9.6.4.30 |
| 9.7[1] | 9.8.4.7 |
| 9.8 | 9.8.4.7 |
| 9.9 | 9.9.2.50 |
| 9.10 | 9.10.1.22 |
| 9.12 | 9.12.2 |

[1] Cisco ASA ソフトウェアの 9.4 より前のリリース、Cisco ASA ソフトウェア リリース 9.5、および 9.7 については、メンテナンスが終了しています。 この脆弱性に対する修正を含むサポート対象リリースに移行することをお勧めします。

# 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

シスコは、この脆弱性について報告してくださった Nirvan 氏のチームに感謝いたします。

## URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-asa-privescala

## 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 8 月 7 日 |

## 利用規約