Cisco Secure Firewall適応型セキュリティアプライアンスソフトウェア、Secure Firewall Threat Defenseソフトウェア、IOSソフトウェア、IOS XEソフトウェア、およびIOS XRソフトウェアWebサービスのリモートコード実行の脆弱性

アドバイザリーID : cisco-sa-http-code-exec-WmfP3h3O
初公開日 : 2025-09-25 16:00
バージョン 1.0 : Final
CVSSスコア : 9.0
回避策 : No workarounds available
Cisco バグ ID : CSCwo35704 CSCwo18850 CSCwo35779 CSCwo49562
CVE-2025-20363

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 Secure Firewall Adaptive Security Appliance(ASA)ソフトウェア、Cisco Secure Firewall Threat Defense(FTD)ソフトウェア、Cisco IOSソフトウェア、Cisco IOS XEソフトウェア、およびCisco IOS XRソフトウェアのWebサービスの脆弱性により、認証されていないリモート攻撃者（Cisco ASAおよびFTDソフトウェア）または低ユーザ権限を持つ認証されたリモート攻撃者（Cisco IOS、IOS XE、およびIOS XRソフトウェア）が該当デバイスでの任意のコードを実行する実行する可能性があります。

この脆弱性は、HTTP要求でのユーザ入力の検証が不適切なことに起因します。攻撃者は、システムに関する追加情報を取得した後で、巧妙に細工されたHTTP要求を該当デバイスのターゲットWebサービスに送信するか、不正利用の影響を緩和するか、またはその両方を試すことで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はrootとして任意のコードを実行し、該当デバイスが完全に侵害される可能性があります。

この脆弱性の詳細については、このアドバイザリの「詳細情報」のセクションを参照してください。

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おり、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強く推奨します。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-http-code-exec-WmfP3h3O

このアドバイザリで説明されている脆弱性の詳細については、『Cisco Event Response: Continued Attacks Against Cisco Firewall Platforms』を参照してください。

該当製品

脆弱性のある製品

本脆弱性は、以下のシスコ製品に影響します。

- Secure Firewall ASA SoftwareおよびSecure Firewall FTD Softwareを参照してください。(CSCwo18850)
- IOSソフトウェア（リモートアクセスSSL VPN機能が有効な場合）(CSCwo35704)
- IOS XEソフトウェア（リモートアクセスSSL VPN機能が有効な場合）(CSCwo35704、CSCwo35779)
- IOS XRソフトウェア（32ビット）（HTTPサーバが有効なCisco ASR 9001ルータで実行されている場合）(CSCwo49562)

脆弱性が存在する Cisco 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」セクションを参照してください。

デバイス設定の確認

デバイスに脆弱な設定があるかどうかを確認するには、次のソフトウェア固有のセクションを参照してください。

Cisco Secure Firewall ASAソフトウェア

次の表では、左列に潜在的脆弱性のある Cisco Secure Firewall ASA ソフトウェアの機能を記載しています。また右の列には、show running-config CLI コマンドで判断可能な、この機能の基本設定を示します。これらの機能により、SSL リスニングソケットが有効になる可能性があります。

Cisco Secure Firewall ASA ソフトウェアの機能	脆弱性の可能性がある設定
モバイル ユーザ セキュリティ（MUS）	webvpn mus password mus server enable port *<Port_number>* mus *<IPv4_address>* *<IPv4_mask>* *<interface_name>*

Cisco Secure Firewall ASA ソフトウェアの機能	脆弱性の可能性がある設定
SSL VPN	webvpn enable <*interface_name*>

Cisco Secure Firewall FTDソフトウェア

次の表では、左の列に、脆弱性が存在する可能性のあるCisco Secure Firewall FTDソフトウェアの機能を示しています。また右の列には、show running-config CLI コマンドで判断可能な、この機能の基本設定を示します。これらの機能により、SSL リスニングソケットが有効になる可能性があります。

Cisco Secure FTD ソフトウェアの機能	脆弱性の可能性がある設定
AnyConnect SSL VPN	webvpn enable <*interface_name*>

リモートアクセスVPN機能は、Cisco Secure Firewall Management Center(FMC)ソフトウェアのDevices > VPN > Remote Access、またはCisco Secure Firewall Device Manager(FDM)のDevice > Remote Access VPNで有効になっています。

Cisco IOS ソフトウェア

リモートアクセスSSL VPN機能が有効になっているかどうかを確認するには、show running-config | section webvpn CLIコマンドを使用します。次の例に示すように、デバイスから別の行にinserviceコマンドが含まれる出力が返される場合、リモートアクセスSSL VPN(WebVPN)が設定されており、デバイスはこの脆弱性の影響を受けます。

<#root>

```
Router#
```

show running-config | section webvpn

```
webvpn gateway ssl-vpn
 ip address 192.168.100.1 port 443
 ssl trustpoint WebVPN-TP
```

```
inservice

 !
Router#
```

Cisco IOS XE ソフトウェア

リモートアクセスSSL VPN機能が有効になっているかどうかを確認するには、show running-config | section crypto ssl policy CLIコマンドを使用します。次の例に示すように、デバイスから別の行にshutdownコマンドが含まれていないポリシーが返された場合、リモートアクセスSSL VPNが設定されており、デバイスがこの脆弱性の影響を受けます。

```
<#root>

Router#

show running-config | section crypto ssl policy


crypto ssl policy policy1
 ssl proposal proposal1
 pki trustpoint TP-self-signed-1057422294 sign
 ip address local 10.0.0.1 port 443
Router#
```

Cisco IOS XR ソフトウェア

Cisco IOS XRソフトウェアが32ビット用かどうかを確認するには、run uname -s CLIコマンドを使用します。そのコマンドの出力にQNXが含まれている場合、デバイスは32ビットベースです。64ビットベースのシステムにはLinuxが含まれます。

次の例は、32ビットデバイスでのrun uname -sコマンドの出力を示しています。

```
<#root>

RP/0/RSP0/CPU0:ASR-9001#

run uname -s


Mon Sep  8 13:17:27.464 UTC

QNX


RP/0/RSP0/CPU0:ASR-9001#
```

run uname -sコマンドでLinuxという出力が返される場合、そのデバイスは、この脆弱性の影響を受けません。ただし、コマンドによって出力QNXが返される場合、HTTPサーバが有効になっていれば、デバイスはこの脆弱性の影響を受ける可能性があります。

注：32ビットと64ビットCisco IOS XRソフトウェアの詳細については、「Cisco IOS XR 32ビットOSと64ビットOSの違い」を参照してください。

HTTP機能が有効になっているかどうかを確認するには、show running-config | include http server CLIコマンドを使用します。このコマンドで出力が返された場合、HTTPサーバが有効になっており、このデバイスはこの脆弱性の影響を受ける可能性があります。次に例を示します。

```
<#root>

RP/0/RSP0/CPU0:ASR-9001#

show running-config | include http server


Mon Sep  8 11:57:45.667 UTC
Building configuration...

http server


RP/0/RSP0/CPU0:ASR-9001#
```

show running-config | include http serverコマンドで空の出力が返される場合、そのデバイスはこの脆弱性の影響を受けません。

run uname -sコマンドでQNXが返され、show running-config | include http serverコマンドで出力が返される場合、デバイスはこの脆弱性の影響を受けます。

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のある製品セクションにリストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性が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 Secure Firewall ASAおよびSecure Firewall FTDソフトウェア

Cisco Secure Firewall ASAソフトウェアおよびCisco Secure FTDソフトウェアのWebサービスの脆弱性により、認証されていないリモートの攻撃者が該当デバイスで任意のコードを実行する可能性があります。

セキュリティ影響評価（SIR）：致命的
CVSS ベーススコア：9
CVSS ベクトル：CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Cisco IOS、IOS XE、およびIOS XRソフトウェア

Cisco IOSソフトウェア、Cisco IOS XEソフトウェア、およびCisco IOS XRソフトウェアのWebサービスにおける脆弱性により、ユーザ権限の低い認証されたリモート攻撃者が該当デバイスで任意のコードを実行する可能性があります。

セキュリティ影響評価（SIR）：高
CVSS ベーススコア：8.5
CVSSベクトル：CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

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

シスコでは、修正済みソフトウェアリリースへのアップグレードが利用可能になるまで、回避策や緩和策は一時的な解決策であると考えています。この脆弱性を完全に修復し、本アドバイザリで説明されている障害の発生を回避するために、お客様には本アドバイザリで説明されている修正済みソフトウェアにアップグレードすることを強く推奨します。

Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェア

お客様が Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェアにおける脆弱性のリスクの有無を判断できるように、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。 また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべて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。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。すべてのアドバイザリ、セキュリティへの影響の評価（SIR）が「重大」または「高」のアドバイザリのみ、またはこのアドバイザリのみを選択します。
2. 該当するソフトウェアを選択します。

3. 該当するプラットフォームを選択します。
4. リリース番号を入力します。たとえば、Cisco Secure Firewall ASA ソフトウェアの場合は 9.20.3.4、Cisco Secure FTD ソフトウェアの場合は 7.4.2 と入力します。
5. [チェック（Check）] をクリックします。

2 | Critical,High,Medium
このアドバイザのみ | Cisco ASA ソフトウェア
あらゆるプラットフォーム

Enter release number | Check

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS 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に、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべて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。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。あるいは、次のフォームを使用して、シスコ セキュリティ アドバイザリに該当するリリースであるかどうかを確認します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. リリース番号（例：15.9(3)M2、17.3.3）を入力します。
3. [チェック（Check）] をクリックします。

2 | Critical,High,Medium
このアドバイザのみ

Enter release number | Check

Cisco IOS XR ソフトウェア

次の表では、最初の列にシスコソフトウェアリリースまたはトレインを示します。2番目の列は影響を受けるプラットフォームを示します。3番目の列は、影響を受けるアーキテクチャを示します。右の列は、このアドバイザリに記載されている脆弱性の影響を受けるリリース（トレイン）の

修正を要求する方法を示しています。

Cisco IOS XR ソフトウェア リリース	Platform	アーキテクチャ	SMU 名
6.8	ASR 9001	32ビット	適切なサポート組織に連絡し、SMUを要求します。
6.9	ASR 9001	32ビット	適切なサポート組織に連絡し、SMUを要求します。

シスコの Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、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は確認しておりません。

出典

この脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のKeane O'Kelley氏によって、Cisco TACサポートケースの解決中に発見されました。

シスコは、この調査をサポートしていただいた次の組織に感謝いたします。

- オーストラリア信号局オーストラリアサイバーセキュリティセンター
- カナダのサイバーセキュリティセンター（通信セキュリティ施設の一部）
- 英国National Cyber Security Center(NCSC)
- 米国サイバーセキュリティおよびインフラストラクチャセキュリティ機関(CISA)

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http-code-exec-WmfP3h3O

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	2025年9月25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。

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。