シスコ製品に影響を与える Apache HTTP サーバーの複数の脆弱性2021 年 11 月

High

アドバイザリーID : cisco-sa-apache-httpd-2.4.49-VWL69sWQ

初公開日 : 2021-11-24 16:00

最終更新日 : 2022-01-20 22:52

バージョン 1.8 : Interim

CVSSスコア : 9.0

回避策 : Yes

Cisco バグ ID :

CVE-2021-36160

CVE-2021-40438

CVE-2021-39275

CVE-2021-33193

CVE-2021-34798

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

2021 年 9 月 16 日、Apache ソフトウェア財団は、Apache HTTP サーバー（httpd）の 2.4.48 以前のリリースに影響を与える 5 つの脆弱性を開示しました。

これらの脆弱性の説明については、Apache HTTP サーバー 2.4 脆弱性 Web ページの Apache HTTP サーバー 2.4.49 セクションを参照してください。

このアドバイザリは追加情報が入手可能になった時点で更新されます。

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-apache-httpd-2.4.49-VWL69sWQ

該当製品

シスコでは、これらの脆弱性の影響を受ける製品を判断するために、製品ラインを調査中です。

調査の進行に伴い、シスコはこのアドバイザリを更新し、影響を受ける製品についてお知らせします。

脆弱性のある製品セクションで、影響を受ける各製品の Cisco Bug ID を示します。Cisco Bug は Cisco Bug Search Tool で検索可能であり、回避策（使用可能な場合）と修正されたソフトウェアリリースなど、プラットフォーム固有の追加情報が記載されます。

調査中の製品

現在、調査中の製品はありません。シスコはこの状況を引き続き監視し、情報が利用可能になった時点でこのドキュメントを更新します。

脆弱性のある製品

次の表に、このアドバイザリに記載された脆弱性の影響を 1 つ以上受けるシスコ製品を示します。将来のソフトウェア リリース日が示されている場合、その日付はこのアドバイザリの上部にある最終更新日時点でシスコが把握しているすべての情報に基づいた日付になります。このソフトウェア リリースの日付は、試験結果や優先される機能や修正の提供等いくつかの理由により変更される場合があります。影響を受けるコンポーネントについてバージョン情報や日付がリストに記載されていない場合（空欄や暫定とされているもの）、シスコは修正の評価を続けており、追加情報が確認された時点でアドバイザリを更新します。アドバイザリが Final とマークされた後、より詳細な情報については関連する Cisco バグを参照して下さい。

Product	Cisco Bug ID	Fixed Release Availability
ネットワーク アプリケーション、サービス、およびアクセラレーション		
Cisco Cloud Services Platform 2100	CSCwa33065	2.8.2 (Apr 2022)
Cisco Wide Area Application Services（WAAS）	CSCwa33076	6.4.5d（2022 年 4 月）
ネットワークおよびコンテンツ セキュリティ デバイス		
Firepower 4100/9300 シリーズ アプライアンス用 Cisco FXOS ソフトウェア	CSCvz91266	2.9.1（使用可能） 2.10.1（使用可能） 2.11.1（使用可能） 2.12.1 (Apr 2022)
Cisco Firepower Management Center[1]	CSCvz91270	7.0.2 (May 2022) 7.1.0.1 (May 2022)
Cisco Firepower 次世代侵入防御システム（NGIPS）[1]	CSCwa15291	6.4.0.14 (May 2022) 6.6.7（2022 年 3 月）
Cisco Firepower Management Center によって管理される Cisco Firepower Threat Defense（FTD）[1]	CSCwa15291	6.4.0.14 (May 2022) 6.6.7（2022 年 3 月）
ネットワーク管理とプロビジョニング		
Cisco Policy Suite[1]	CSCwa33078	22.1（2022 年 3 月）
Cisco Prime Collaboration Provisioning	CSCwa33069	計画なし
Cisco Prime Infrastructure	CSCvz83342	3.10（利用可能）
Cisco Prime Opticalサービス プロバ	CSCwa33067	アップグレードオプションについては、Cisco

イダー向け		TAC にお問い合わせください。
Cisco Security Manager	CSCwa33073	4.25 (Jun 2022)
ルーティングおよびスイッチング - エンタープライズおよびサービス プロバイダー		
Cisco Network Assurance Engine[1]	CSCwa16137	6.0.1（使用可能）
Unified Computing		
Cisco UCS Central ソフトウェア	CSCwa33066	
Cisco UCS Director ベアメタルエージェント[1]	CSCwa33064	6.8.1.1（2022 年 2 月）
Cisco UCS Manager	CSCwa33718	
ビデオ、ストリーミング、テレプレゼンス、およびトランスコーディング デバイス		
Cisco Expressway Series	CSCwa01545	14.0.4（使用可能） 14.1（リリース予定）
Cisco Meeting Server	CSCwa58708	3.5 (May 2022) 3.4 (Feb 2022) 3.3（2022年3月） 3.2（2022年3月）
Cisco TelePresence Video Communication Server（VCS）	CSCwa01545	14.0.4（使用可能） 14.1（リリース予定）
ワイヤレス		
LoRaWAN 向けシスコ ワイヤレス ゲートウェイ	CSCwa33724	2.3.1（2022年3月）
シスコ クラウド ホステッド サービス		
Cisco Smart Net Total Care - On-Premises	CSCwa33060	2.2.1（2022年3月）

1. この製品は CVE-2021-40438 に対して脆弱です。

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記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。

シスコは、これらの脆弱性が以下の製品には影響を与えないことを確認しました。

ネットワーク アプリケーション、サービス、およびアクセラレーション

- Cisco Nexus 1000VE シリーズ仮想スイッチ

ネットワークおよびコンテンツ セキュリティ デバイス

- Cisco Secure Network Analytics（旧 Stealthwatch）

ネットワーク管理とプロビジョニング

- Cisco Prime Collaboration Assurance
- Cisco Prime Network Services Controller
- Cisco Virtual Topology System

ルーティングおよびスイッチング - エンタープライズおよびサービス プロバイダー

- Cisco DNA Center

Unified Computing

- Cisco Virtual Security Gateway

音声およびユニファイド コミュニケーション デバイス

- Cisco Hosted Collaboration Mediation Fulfillment
- Cisco SocialMiner
- Cisco Unified Communications Domain Manager
- Cisco Unified Communications Manager および Cisco Unified Communications Manager セッション管理エディション
- Cisco Unified Communications Manager IM & Presence Service
- Cisco Unified Contact Center Express

ビデオ、ストリーミング、テレプレゼンス、およびトランスコーディング デバイス

- Cisco Video Surveillance Media Server

シスコ クラウド ホステッド サービス

- Cisco Smart Software Manager オンプレミス

回避策

すべての回避策は、製品固有の Cisco Bug として文書化され、それぞれこのアドバイザリの「脆弱性のある製品」セクションで特定されます。

修正済みソフトウェア

修正済みソフトウェア リリースの詳細については、本アドバイザリの「脆弱性のある製品」セクションに記載されている Cisco Bug ID を参照してください。

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 セキュリティ アドバイザリ 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アップグレード ソリューション一式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。

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

2021 年 11 月、Cisco PSIRT は、CVE ID CVE-2021-40438 で識別される脆弱性のエクスプロイトが試みられたことを認識しました。

出典

これらの脆弱性は、2021 年 9 月 16 日に Apache ソフトウェア財団によって公開されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-httpd-2.4.49-VWL69sWQ

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.8	概要を更新。調査中の製品、脆弱性のある製品、脆弱性を含んでいないことが確認された製品のリストを更新。	要約, 該当製品, 脆弱性が存在する製品, 脆弱性が存在しないことが確認された製品	Interim	2022年1月20日
1.7	「調査中の製品」、「脆弱性のある製品」、「脆弱性が存在しないことが確認された製品」を更新。Cisco Security Manager の修正リリースのリリース日を修正。	該当製品	Interim	2021 年 12 月 16 日
1.6	調査中の製品、脆弱性のある製品、脆弱性を含んでいないことが確認された製品のリストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含んでいないことが確認された製品	Interim	2021 年 12 月 8 日
1.5	調査中の製品および脆弱性が存在する製品のリストを更新。	「該当製品」、「脆弱性のある製品」	Interim	2021 年 12 月 03 日
1.4	調査中の製品、脆弱性のある製品、脆弱性を含んでいないことが確認された製品のリストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含んでいないことが確認された製品	Interim	2021 年 12 月 02 日
1.3	調査中の製品、脆弱性のある製品、脆弱性を含んでいないことが確認された製品のリストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含んでいないことが確認された製品	Interim	2021 年 12 月 01 日
1.2	脆弱性を含んでいないことが確認された製品のリストを追加。脆弱性のある製品と調査中の製品のリストを	該当製品, 脆弱性が存在する製品, 脆弱	Interim	2021 年 11

	更新。	性を含んでいないことが確認された製品		月 26 日
1.1	調査中の製品のリストを追加。脆弱性のある製品のリストを更新。	該当製品および脆弱性のある製品	Interim	2021 年 11 月 25 日
1.0	初回公開リリース	—	Interim	2021-NOV-24

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。