Axis脆弱性管理ポリシー

概要

CVE採番機関 (CNA) として、Axisは、自社製品で発見されたセキュリティ脆弱性の管理と対応において業界のベストプラクティスに従っています。ただし、Axisが提供する製品やサービスに脆弱性が皆無であることを保証することはできません。これはAxisに限ったことではなく、すべてのソフトウェアとサービスに共通する条件です。Axisが保証できるのは、*開発の各段階*で潜在的な脆弱性を特定し、軽減するために最大限の努力を尽くすことで、お客様の環境にAxis製品やサービスを導入する際のリスクを最小限に抑えることです。

Axisは、特定の標準ネットワークプロトコルやサービスに、悪用される可能性のある固有の脆弱性が存在する可能性があることを認識しています。Axisはこれらのプロトコルやサービスについて責任を負いませんが、Axisの製品、ソフトウェア、サービスに関連するリスクを軽減するための推奨事項を、*AXIS OS 強化ガイド*、*AXIS Camera Station システム強化ガイド*、*Axis Network Switch 強化ガイド*という形で提供しています。

対象

本ドキュメントに記載されている脆弱性管理ポリシーは、*Axisブランドのすべての製品*、ソフトウェア、サービスに適用されます。このポリシーの対象外となるのは、*2Nセキュリティチーム*が管理する2N製の製品、ソフトウェア、サービスです。

コミットメント

Axisは、Axisの製品、ソフトウェア、およびサービスの脆弱性を特定し報告する研究者の努力を高く評価し、奨励しています。責任ある開示プロセスに従うことで、Axis製品セキュリティチームは、できる限り、開示プロセス全体にわたる相互協力と透明性を通じて研究者の利益を尊重します。

Axisは、研究者が90日間または相互に合意した期日より前に脆弱性を公開しないこと、また、Axisとそのパートナーおよび顧客に危害を与えたり、プライバシーを漏洩したり、安全を損なったりしない法的範囲内で脆弱性調査を実施するよう求めています。

脆弱性の管理

Axisは、*サードパーティ製のオープンソースコンポーネント*とAxis固有の脆弱性に対して同じ分類を使用します。脆弱性は、一般に知られている*共通脆弱性評価システム* (CVSS) を使用してスコアリングされます。オープンソースの脆弱性に関しては、Axisは自社の製品、ソフトウェア、およびサービスの推奨導入方法に基づき、その関連性に応じて脆弱性を評価する場合があります。セキュリティアドバイザリは通常、Axis固有の脆弱性に対してのみ提供されます。以下のセクションでは、脆弱性が評価され、修正の対象となる場合の優先順位について説明します。

CVSS v4.0 高/緊急 (7.0～10.0)

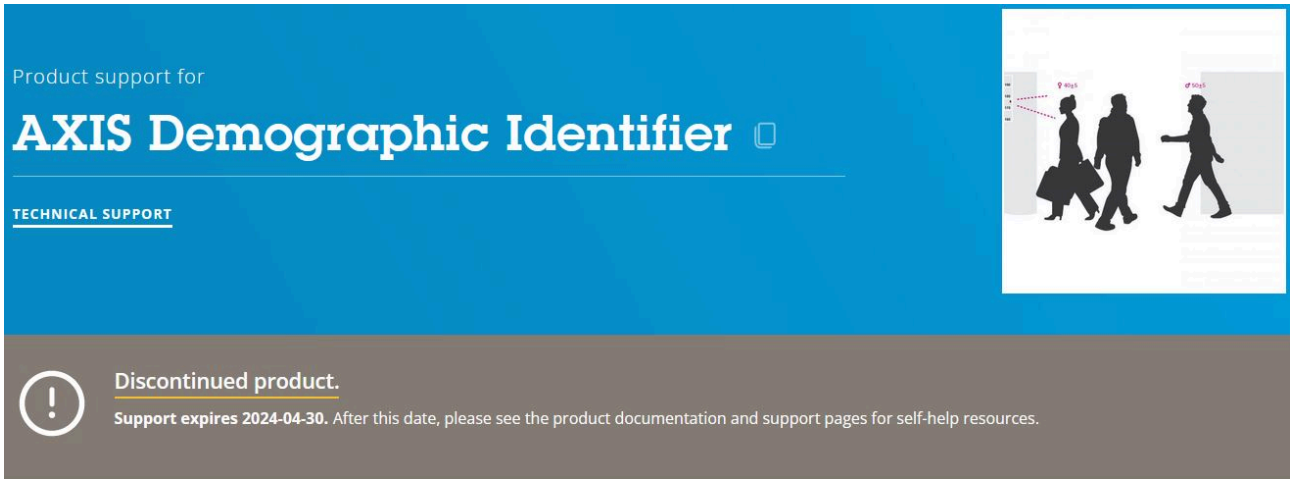
Axisは、外部への公開後4週間以内に脆弱性を解決することを目指しています。オープンソースコンポーネントの場合、Axisは情報、パッチ、検証などを外部に依存しているため、リードタイムは通常これよりも長くなります。脆弱性を解決するには、ソフトウェアのパッチ適用や、影響を受けるコンポーネントや機能の無効化による軽減が必要になります。

CVSS v4.0 低/中 (0.1～6.9)

低／中レベルの脆弱性は、通常、デバイスへの特権アクセスを必要とするか、機密性・完全性・可用性への影響が限定的であるため、製品のセキュリティへの影響は比較的軽微です。したがって、Axisは、必要と判断した場合、今後予定されているリリースの一環として、この脆弱性を解決することがあります。オープンソースコンポーネントの場合、Axisは情報、パッチ、検証などを外部に依存しているため、リードタイムは通常これよりも長くなります。脆弱性を解決するには、ソフトウェアのパッチ適用や、影響を受けるコンポーネントや機能の無効化による軽減が必要になります。

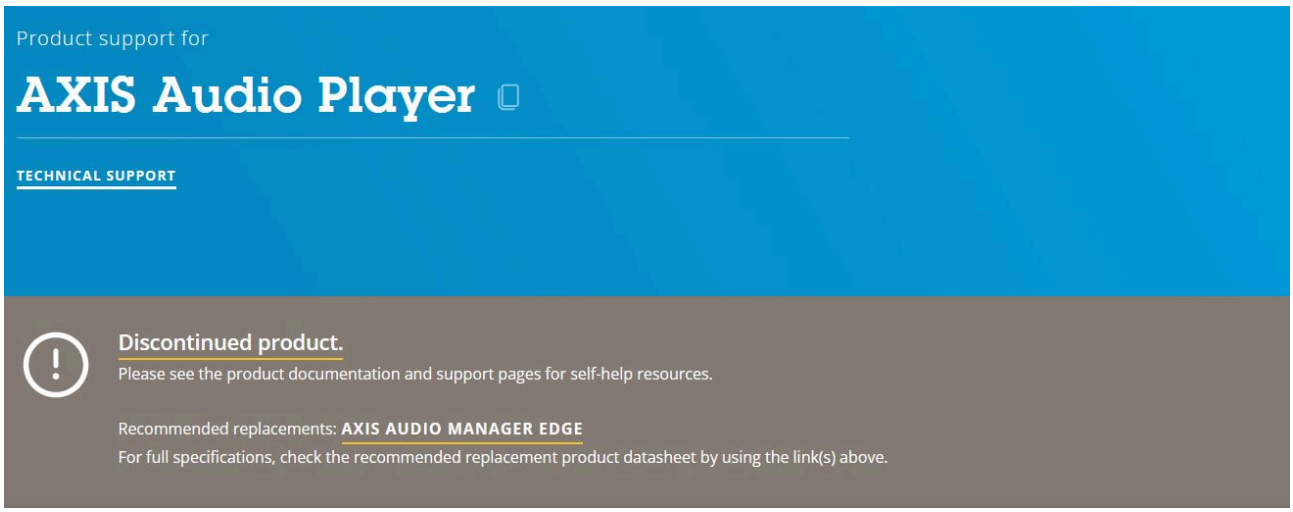
サポートされるソフトウェア/サービス

Axisのソフトウェアやサービスのサポート提供段階は、共通のソフトウェアライフサイクルプロセスに基づいて定義されています。Axisのソフトウェアとサービスは通常、販売終了日から3年間サポートされます。



2024年4月30日までサポートが提供される販売終了ソフトウェア製品の例。

このフェーズにある間は、Axisのソフトウェア/サービスは、販売終了ソフトウェア/サービスの段階に達するまでサポートされると見なされます。

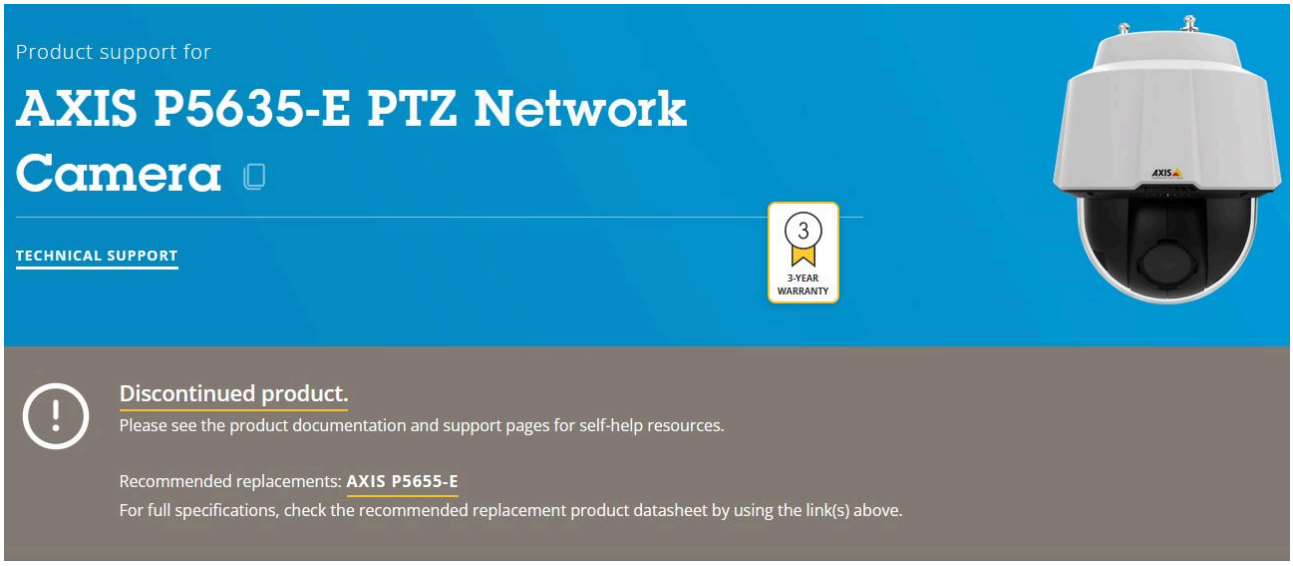


axis.comに掲載されている販売終了ソフトウェア製品の例。

サポート対象製品

Axis製品のサポートは、共通のハードウェア製品ライフサイクルプロセスに基づいて定義されています。Axis製品は、販売終了製品となり、オンラインサポートのみのフェーズに達するまでサポートされると見なされます。

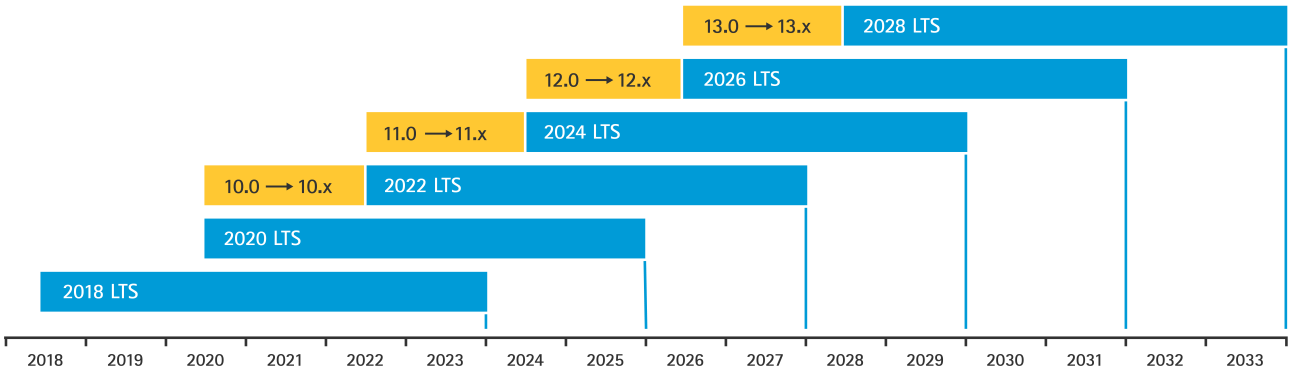
Axis製品の実際のステータスに関する情報は、*www.axis.com*の該当する製品ページから入手できます。製品の販売終了後の一般的なサポートポリシーの詳細については、こちらをご覧ください。



axis.comに掲載されている販売終了ハードウェア製品の例。

AXIS OSは、ほとんどのAxisネットワーク製品に搭載されているオペレーティングシステムです。Axisは、多くの製品に対して、AXIS OSの長期サポート (LTS) トラックを通じて拡張ソフトウェアサポートを提供しています。LTSトラックを利用することで、Axis製品の製品ライフサイクルサポートを延長することができます。AXIS OSについて詳しくは、こちらをご覧ください。

AXIS OSのサポートの概要



アクティブトラックは、2か月ごとに新しいバージョンがリリースされ、最新版のみがサポートされます。LTSトラックは2年ごとに作成され、約5年間サポート・メンテナンスされます。

現在サポートされているAXIS OSのLTSトラックおよびアクティブトラック (2023年10月時点)。

脆弱性の報告

Axisは、提供するサービスの脆弱性に関連するリスクの特定や、最小限に抑えるための取り組みを継続的に行っています。ただし、Axisの製品、ソフトウェア、またはサービスに関連するセキュリティの脆弱性を発見した場合は、ただちに問題を報告してください。セキュリティの脆弱性が実際に悪用される可能性を減らすためには、速やかな報告が重要です。オープンソースのソフトウェアコンポーネントに関するセキュリティの脆弱性は、責任のある組織に直接報告する必要があります。

潜在的な脆弱性を特定したエンドユーザー、パートナー、ベンダー、業界団体、または独立系研究者の皆さまは、速やかに、こちらのフォームを通じてご報告くださいますようお願い致します。提出いただくレポートには、以下の項目を含める必要があります。

- 潜在的な脆弱性に関する技術情報
- 再現手順
- *推定CVSS v4.0スコアとそのベクター文字列*
- 是正策の提案
- 研究者自身の脆弱性開示ポリシー (ある場合)

Axisからの返答に要する時間は以下の通りです。

- 最初の返答までの時間: 初回レポート受け取り後2営業日以内。
- トリアージ: 初回の返答から10営業日以内。

AxisはBugcrowd社と協力し、AXIS OSベースの製品およびAxis Camera Station Proを対象としたバグバウンティプログラム *(脆弱性報奨金制度)* を提供しています。当社はセキュリティ研究者やエシカルハッカーの方のプログラムへの参加を歓迎します。当社独自のバグバウンティプログラムに参加するには、*脆弱性報告プロセス*からリクエストを送信してください。現在、その他のAxisの製品、ソフトウェア、サービスはバグバウンティプログラムの対象外です。

重要な脆弱性の発見に貢献していただいたセキュリティ研究者やエシカルハッカーの方々には、感謝の意を表するため、当社のセキュリティアドバイザリや*Hall of Fame (セキュリティの殿堂)* にお名前を掲載させていただくことがあります。

脆弱性の開示

報告された脆弱性を調査し、正当な脆弱性であることが確認されると、Axisは脆弱性にCVE IDを割り当て、責任ある情報開示プロセスを開始します。Axisは、CVSS v4.0スコア、セキュリティアドバイザリやプレスリリースの内容 (該当する場合)、外部開示の日付など、さらなる詳細について研究者と協力するよう努めています。

Axisと研究者の間で調整を行った後、AxisはCVE IDをMITREに送信し、セキュリティアドバイザリやプレスリリースを公開することで、脆弱性を外部に開示します。

対象外の脆弱性

一部の脆弱性は、Axis脆弱性管理ポリシーの対象外です。以下のリストに記載された対象外の脆弱性については、*product-security@axis.com* にレポートを提出しないでください。

- Microsoft Windows OS上で実行されているAxisソフトウェアアプリケーションにおける**DLLハイジャック/DLLサイドローディングの脆弱性**。詳細については、*こちらの記事*を参照してください。
- **高いアクセス権やソーシャルエンジニアリングを必要とする脆弱性**で、root/管理者権限で開始・実行され、複雑なユーザー操作を必要とするもの。
- 現在使用されていないサービスに向けて設定されたホストの制御を取得するなどの**サブドメインの乗っ取り**。
- 以下のAxis 強化ガイド (Hardening Guide) に従うことで防げた**ユーザーの設定ミス**。
  - *AXIS OSハードニングガイド*
  - *AXIS Camera Station System Hardening Guide*
  - *Axisネットワークスイッチ 強化ガイド*
- Axisデバイスにアップロードして実行できるACAPなど、**サードパーティのユーザーまたはパートナーが作成したコンテンツやアプリケーションの脆弱性**。
- ユーザーを悪意のあるWebサイトにアクセスさせたり、AxisデバイスのWebインターフェースへのアクセス中に偽装されたリンクをクリックさせたりする、**クロスサイトリクエストフォージェリ (CSRF) またはクロスサイトスクリプティング (XSS) の脆弱性**。詳細については、*こちらのセキュリティアドバイザリ*を参照してください。
- **DoSタイプの攻撃**。これには、以下のような攻撃が含まれます。
  - 変更されたパラメーター入力による通常のAPI使用で引き起こされるデバイスのリソース枯渇。
  - 高頻度のAPI呼び出しによるリソース枯渇。
  - slowloris攻撃によるリソース枯渇。
- Axisの製品、ソフトウェア、サービスで使用されるソフトウェアコンポーネントやパッケージに存在するCVE IDで登録された**サードパーティ製オープンソースの脆弱性**。このようなソフトウェアコンポーネントの一般的な例として、Linuxカーネル、OpenSSL、Apacheなどがあります。
- X-Frame-Optionsなどの**HTTP(S)セキュリティヘッダーの欠落**。
- サードパーティ製のネットワークセキュリティスキャナーによって**生成された脆弱性レポート**。
- 「販売終了製品」となった**サポート対象外の製品/ソフトウェア/サービス**。「オンラインサポートのみ」となった製品。

セキュリティ通知サービス

Axisは、ガイドライン、セキュリティアドバイザリ、そして*Axis脆弱性管理ポリシー*に関する声明を公開しています。さらに、*Axisセキュリティ通知サービス*に登録することで情報を入手することができます。

Axis固有の脆弱性については、CVSS v4.0スコアに関係なく通知が送信されます。Axisが分析した脆弱性は、*AXIS OS セキュリティアドバイザリ*に記載されています。