Axis Vulnerability management policy

Overview

As CVE-numbering authority (CNA), Axis adheres to industry best practices in managing and responding to security vulnerabilities discovered in our products. However, there's no way to guarantee that products and services delivered by Axis are entirely free from vulnerabilities. This is not unique to Axis, but rather a general condition for all software and services. What Axis can guarantee is that we will make a concerted effort *at every stage of development* to identify and mitigate potential vulnerabilities, thus minimizing the risk associated with deploying Axis products and services in customer environments.

Axis acknowledges that certain standard network protocols and services may have inherent weaknesses that could be exploited. While Axis does not take responsibility for these protocols and services, we do provide recommendations on how to reduce risks related to your Axis products, software and services in the form of our *AXIS OS Hardening Guide*, *AXIS Camera Station System Hardening Guide*, and *Axis Network Switches Hardening Guide*.

Scope

The vulnerability management policy described in this document applies to all *Axis-branded products, software and services*. Excluded from this policy are 2N products, software and services, which are managed by the *2N security team*.

Commitment

Axis appreciates and encourages the efforts made by researchers in identifying and reporting vulnerabilities in Axis products, software and services. By following the responsible disclosure process, the Axis Product Security Team, to its best abilities, will respect the researcher's interest through mutual collaboration and transparency throughout the disclosure process.

Axis expects researchers not to disclose vulnerabilities before a 90-day period or mutually agreed date and to perform vulnerability research within legal boundaries that would not cause harm, expose privacy, or compromise safety of Axis and its partners and customers.

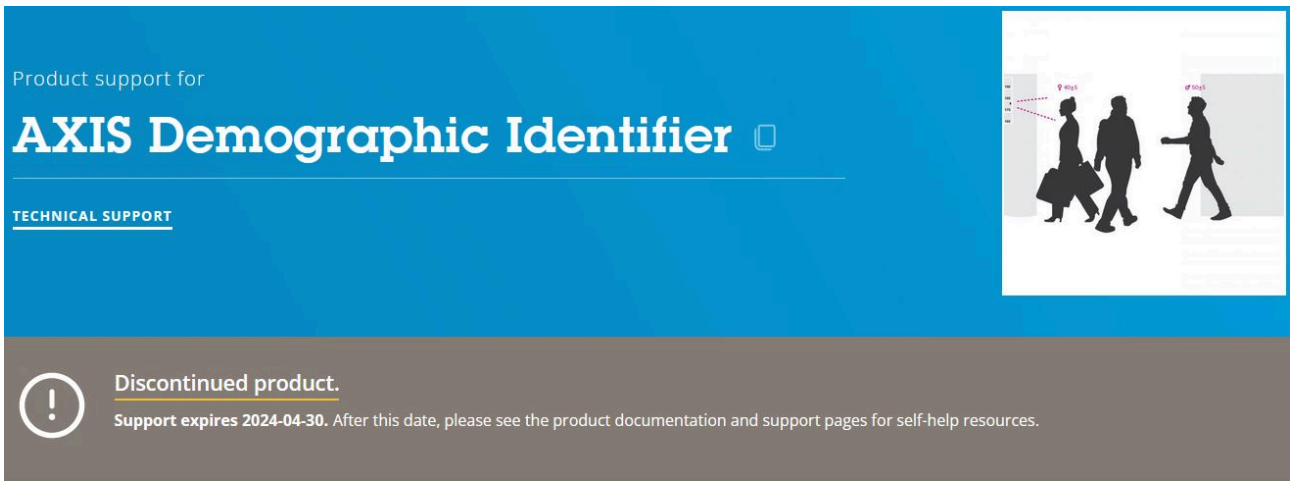
Vulnerability management

Axis uses the same classification for *third-party open-source components* and Axis-specific vulnerabilities. Vulnerabilities are scored using the commonly known *Common Vulnerability Scoring System* (CVSS). With regards to open-source vulnerabilities, Axis may assess the vulnerability according to its relevance in terms of how Axis recommends deploying its products, software, and services. A security advisory is typically provided only for Axis-specific vulnerabilities. The following section describes the prioritization for when a vulnerability has been assessed and is eligible for correction:

CVSS v4.0 high/critical (7.0 – 10.0)
Axis aims to resolve the vulnerability no later than 4 weeks after the external disclosure. For open-source components, the lead-time is usually longer as Axis depends on external parties for information, patches, and/or verification. Resolving a vulnerability either entails patching the software or mitigating the vulnerability by disabling the affected component or functionality.

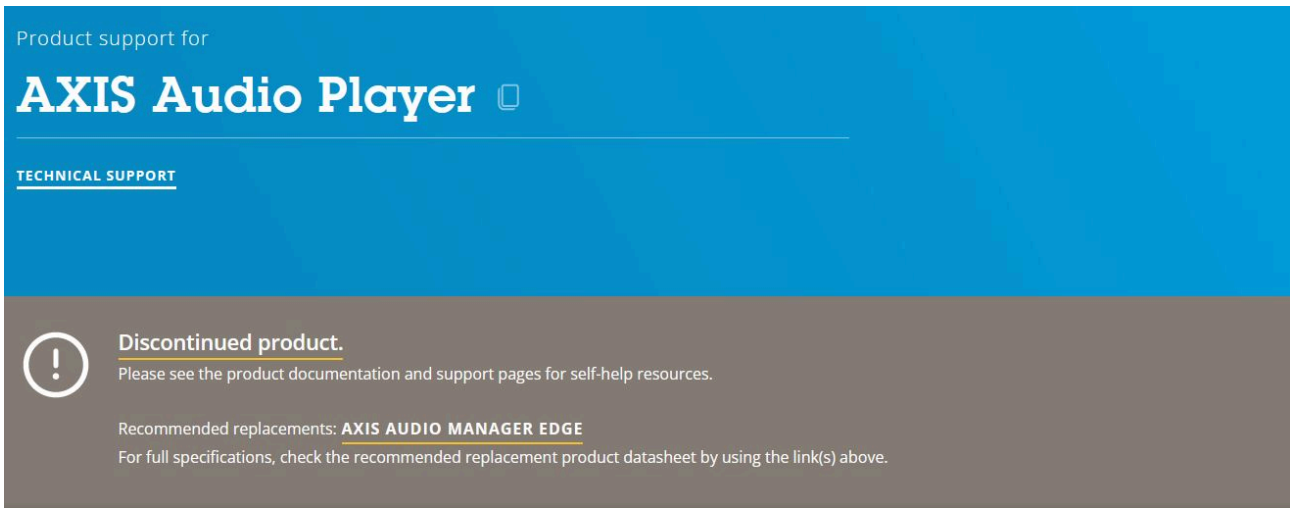
CVSS v4.0 low/medium (0.1 – 6.9)
Low/Medium vulnerabilities typically entail less significant consequences to the product's security as they either require privileged access to the device or have limited impact on confidentiality, integrity, or availability. Therefore, Axis may resolve the vulnerability eventually as part of an upcoming scheduled release if deemed necessary. For open-source components, the lead-time is usually longer as Axis depends on external parties for information, patches, and/or verification. Resolving a vulnerability either entails patching the software or mitigating the vulnerability by disabling the affected component or functionality.

Supported software/services
The support stage of an Axis software/service is defined through a common software lifecycle process. Axis software/services are usually supported three years after the discontinuation announcement.



Example of a discontinued software product that is receiving support until 2024-04-30.

While in this phase, Axis software/services are considered supported until they have reached their Discontinued software/services phase.



Example of a discontinued software product as can be found on axis.com.

Supported products

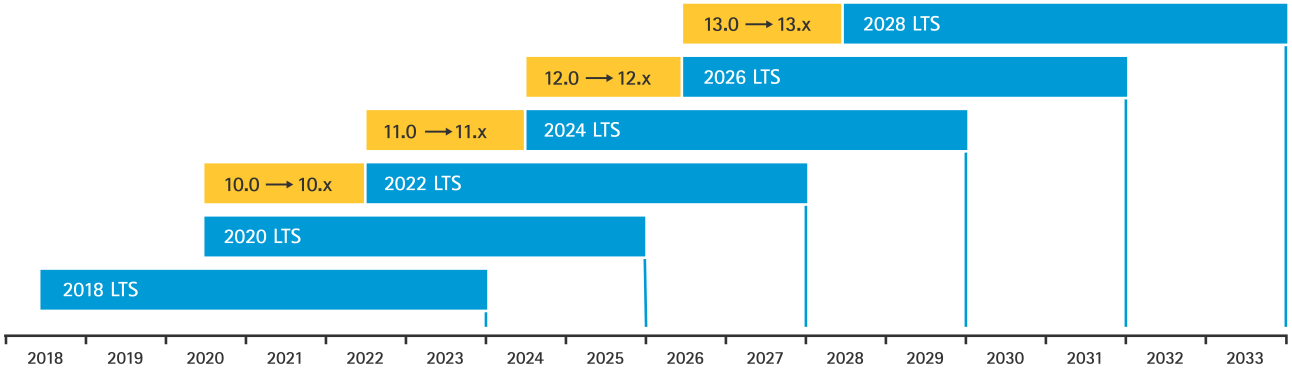
The support of an Axis product is defined through the common *hardware product lifecycle process*. Axis products are considered supported until they have reached the Discontinued product. Online support only phase

Information about the actual status of Axis products can be obtained from the corresponding Axis product page on *www.axis.com*. More information about the general support policy after a product discontinuation can be found *here*.

Example of a discontinued hardware product as can be found on axis.com.

AXIS OS is the operating system that powers most Axis network products. For many products, Axis provides extended software support through AXIS OS long-term support (LTS) tracks. Utilizing the LTS track can extend the overall product lifecycle support of an Axis product. Read more about AXIS OS *here*.

AXIS OS support overview



The active track releases a new version every second months where only the latest version is supported. The LTS tracks are created every two years and are supported and maintained for about 5 years.

Currently supported AXIS OS LTS and active tracks (as of October 2023).

Reporting vulnerabilities

Axis works continuously to identify and limit the risk associated with vulnerabilities in our offering. However, if you identify a security vulnerability associated with an Axis product, software or service, we urge you to report the problem immediately. Timely reporting of security vulnerabilities is critical for reducing the likelihood that they can be exploited in practice. Security vulnerabilities related to open-source software components should be addressed directly to the responsible entity.

End users, partners, vendors, industry groups, and independent researchers who have identified a potential vulnerability are encouraged to submit their findings through *this form*. The submitted report should include:

- Technical information about the potential vulnerability.
- Steps to reproduce.
- *Estimated CVSS v3.1 score rating and resulting vector string*.
- A remediation suggestion.
- The researcher's own vulnerability disclosure policy if available.

The following response times from Axis can be expected:

- The time to first response within 2 business days after receiving the initial submission.
- The time to triage (from the time to first response) within 10 business days.

Axis collaborates with Bugcrowd to offer *Bug Bounty Programs* for AXIS OS-based products. We invite security researchers and ethical hackers to participate in these programs. To join our private bug bounty program, submit a request through the *vulnerability reporting process*. Other Axis products, software, and services are currently not part of any bug bounty program.

As a token of appreciation, security researchers and ethical hackers who contribute valuable findings may receive public recognition in our security advisories and the *Hall of Fame*.

Disclosing vulnerabilities

Once a reported finding has been investigated and confirmed as a legitimate vulnerability, Axis assigns a CVE ID and begins the responsible disclosure process. Axis strives to collaborate with security researchers on further details, such as the CVSS v3.1 score, the content of the security advisory and/or press releases (if applicable), and agrees on the external disclosure date.

Axis follows a structured quarterly CVE disclosure cycle, occurring on the second Tuesday of February, May, August, and November. This schedule serves as the standard window for publicly disclosing validated vulnerabilities, which includes the submission of the CVE ID to MITRE and the publication of the security advisory or press release for the affected Axis products and services. Out-of-band disclosures may be made if deemed necessary. Disclosures are only made when there are CVEs to disclose.

Out-of-scope vulnerabilities

Some vulnerabilities are out-of-scope for the Axis vulnerability management policy. Please do not submit reports on out-of-scope vulnerabilities in the list below to *product-security@axis.com*.

- **DLL-hijacking/DLL-sideloading vulnerabilities** in Axis software applications that are running on Microsoft Windows OS. For more information, see the *following article*.
- **Vulnerabilities requiring high privileges and/or social engineering** that are started/executed with root/administrator access and/or require complex user interactions.
- **Sub-domain takeovers** such as gaining control over a host that points to a service not currently in use.
- **User misconfigurations** that could be prevented by following Axis hardening guides:
  - *AXIS OS Hardening Guide*
  - *AXIS Camera Station System Hardening Guide*
  - *Axis Network Switches Hardening Guide*
- **Vulnerabilities in third party user- or partner-created content or applications**, for instance ACAPs that can be uploaded and run on Axis devices.
- **Cross-site request forgery (CSRF) or cross-site scripting (XSS) vulnerabilities** that trick the user into accessing a malicious website or clicking on a disguised link while accessing the web interface of Axis devices. For more information, see the *following security advisory*.
- **Any DoS type attack**, examples of these are:
  - Resource exhaustion of a device through normal API usage with modified parameter inputs.
  - Resource exhaustion due to high frequency API calls.
  - Resource exhaustion using slowloris attacks.
- **Third party open-source vulnerabilities** that are registered with a CVE ID located in software components or packages used in Axis products, software or services. Common examples of such software components are the Linux Kernel, OpenSSL, Apache, and others.
- **Missing HTTP(S) security headers** such as X-Frame-Options.
- **Vulnerability reports generated** by third party network security scanners.
- **Unsupported products/software/services** that have reached the "Discontinued product. Online support only" phase.
- **Reported issues that do not clearly document a real, exploitable issue with security impact.** For instance, mismatching application-level errors and HTTP response codes when performing API fuzzing.

Security notification service

Axis publishes guidelines, security advisories and statements on *Axis Vulnerability Management Policy*. Furthermore, information can be obtained by subscribing to Axis security notification service on *Security notification servic*e.

Notifications are sent out for Axis-specific vulnerabilities regardless of their CVSS v4.0 score. Vulnerabilities analyzed by Axis are documented in the *AXIS OS Security Advisories*.

T10185928

2026-01 (M16.2)

© 2022 – 2026 Axis Communications AB