Axis Vulnerability Management Policy

for products, software, and services

March 2022

Table of contents

1. Overview 3
2. Scope 3
3. Vulnerability Management 3
4. Reporting vulnerabilities 5
5. Disclosing vulnerabilities 5
6. Receiving information from Axis 5

1. Overview

Axis, as an CVE Numbering Authority (CNA) under the MITRE domain, follows industry best practices in managing and responding to security vulnerabilities discovered in our products. There is 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 reducing 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 devices in the form of our Axis Hardening Guide.

2. 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.

3. Vulnerability management

Axis uses the same classification for 3rd party open-source components and Axis-specific vulnerabilities. Vulnerabilities are scored using the commonly known CVSS rating system (Common Vulnerability Scoring System). With regards to open-source vulnerabilities, Axis may assess the vulnerability accordingly to its relevance in the context 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:

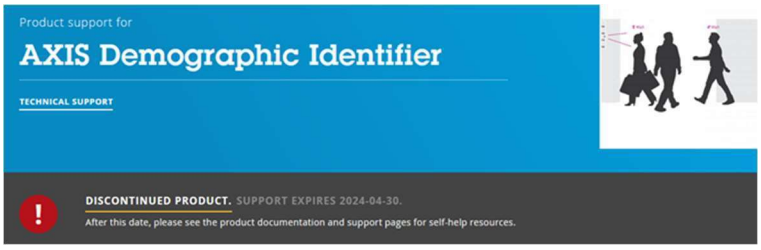
CVSSv3.1 high/critical (7.0 – 10.0)
Axis aims to patch the vulnerability before or within 3 weeks after the external disclosure. For open-source components, the lead-time is usually longer as Axis depends on external parties for information, patches, and/or verification.

CVSSv3.1 medium (4.0 – 6.9)
Axis aims to patch the vulnerability usually within 1 to 3 months.

CVSSv3.1 low (0.1 – 3.9)
Axis aims to patch the vulnerability as part of an upcoming scheduled release.

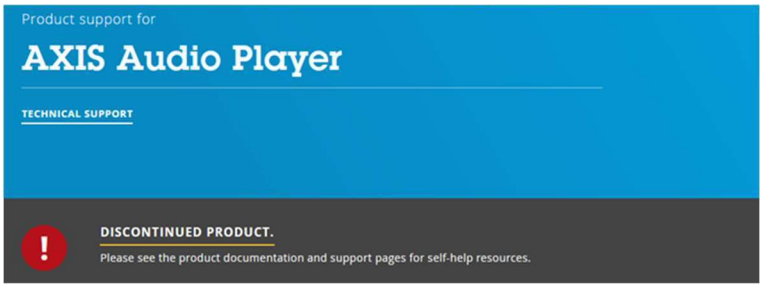
Supported software/services

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 still 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.

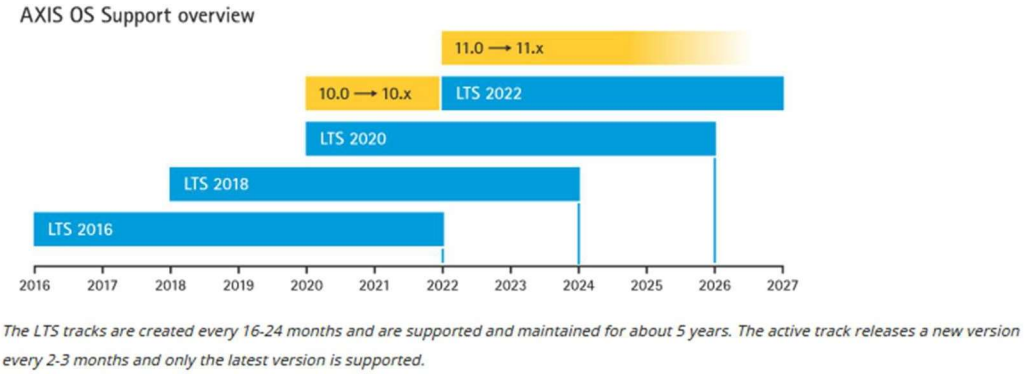
Supported products

The support stage 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 support 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 indication of a discontinued hardware product as can be found on axis.com.

The firmware of an Axis hardware product is referred to as AXIS OS. For many products, Axis provides extended firmware support through Axis OS' long-term support (LTS) tracks. Utilizing the LTS track firmware can extend the overall product-lifecycle support of an Axis product. Read more about AXIS OS here.



Current supported AXIS OS LTS and Active tracks (February 2022).

4. 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 to 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 to product-security@axis.com. The submitted report should include technical information about the potential vulnerability, a remediation suggestion, as well as the reporter's own vulnerability disclosure policy. The reporter can expect a reply from Axis within 48 hours (2 business days) after receiving the initial submission.

Axis does not provide financial reward in the form of a bug bounty program but, if requested by the reporter, Axis may name the reporter in the resulting security advisory to provide appropriate credit for the findings.

5. Disclosing vulnerabilities

Axis expects reporters to perform a responsible disclosure process and not disclose the vulnerability before a 90 day period or mutually agreed date.

After the reported findings have been investigated and validated to be a legitimate vulnerability, Axis assigns a CVE-ID to the vulnerability and initiates the disclosure process. Axis strives to collaborate with the reporter on further details such as the CVSSv3.1 score, the content of the security advisory and/or press releases (if applicable), and the date for the external disclosure.

After alignment between Axis and the reporter, the vulnerability will be externally disclosed by Axis submitting the CVE-ID to MITRE and by publishing the security advisory and/or press release.

6. Receiving information from Axis

Axis publishes guidelines, security advisories and statements on www.axis.com/support/product-security. Furthermore, information can be obtained by subscribing to the Axis security notification on www.axis.com/stay-secure.

Notifications are sent out for Axis-specific vulnerabilities regardless of their CVSSv3.1 score. Notifications for relevant open-source components are sent out for CVSSv3.1 score high and critical (7.0 – 10.0) vulnerabilities. Furthermore, vulnerabilities analyzed by Axis are documented in the AXIS OS Vulnerability Archive.

About Axis Communications

Axis enables a smarter and safer world by creating network solutions that provide insights for improving security and new ways of doing business. As the industry leader in network video, Axisoffers products and services for video surveillance and analytics, access control, and audio systems. Axis has more than 3,500 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Axis was founded in 1984 and has its headquarters in Lund, Sweden.

For more information about Axis, please visit our website www.axis.com.