# AXIS OS Vulnerability Scanner Guide

## Introduction

**AXIS OS Vulnerability Scanner Guide**

for Axis edge devices

**Vulnerabilities and risks**

All software has vulnerabilities that could potentially be exploited. Vulnerabilities will not automatically introduce risk. Risk is defined by the probability of a threat exploiting a vulnerability and the potential negative impact that a successful exploit can do. Reduce any of the two and you reduce the risk. Cybersecurity is about managing risks, and risks are very hard to eliminate. The risk level depends on how a device/software is deployed, operated and managed. Reducing exposure (minimizing the opportunity) is an effective way to mitigate risks. *AXIS OS Hardening Guide* describes several security controls and recommendations for minimizing risks when deploying, operating and maintaining an Axis device.

Some vulnerabilities may be easy to exploit while some may require a high level of sophistication, a special skillset and/or time and determination. A threat requires physical or network access to the device. Some vulnerabilities require administrator privileges to exploit. The CVSS (Common Vulnerability Scoring System) is a commonly used measure to help determine how easy a vulnerability is to exploit and the potential negative impact. These scores are often based on software in critical systems or software that has high exposure to users and/or the Internet. Axis monitors the CVE (Common Vulnerabilities & Exposure) database which publishes known vulnerabilities in software for the CVE entries that relate to the open-source packages used in Axis devices. Vulnerabilities that Axis identifies as limited risk will be remedied in future AXIS OS releases. Vulnerabilities that Axis identifies as an increased risk will be treated with priority resulting in an unscheduled AXIS OS patch or the publishing of a *security advisory* informing about the risk and recommendations.

**Scanning tools reporting false-positives**

Scanning tools will typically try to identify known vulnerabilities by examining version numbers of software and packages found in a device. There is always the possibility that a scanning tool will report a false-positive remark, meaning that the device does not actually have the vulnerability. All remarks from such scanning tools need to be analyzed to validate that they in fact apply to the device. You need to make sure that the Axis device has the latest AXIS OS version as it may include patches that address several vulnerabilities.

### Scope

This guide is written for, and can be applied to, all AXIS OS-based products that are running an AXIS OS LTS or active track. Legacy products running 4.xx and 5.xx versions are also in scope.

**The operating system for Axis edge devices.**

## Quickstart guide

It is recommended to perform regular vulnerability assessments of the infrastructure the Axis device is part of as well as of the Axis device itself. These vulnerability assessments are usually performed by network security scanners. The purpose of a vulnerability assessment is to provide a systematic review of potential security vulnerabilities and misconfigurations. We would like to emphasize the following recommendations before scanning the Axis device for vulnerabilities in order to maximize the quality of the scanning report as well as to avoid common mistakes and false-positives.

- Make sure that the AXIS OS of the device is up to date with the latest available release, either on the AXIS OS long-term support (LTS) track or the active track. The latest available AXIS OS can be downloaded *here*.
- The recommendations in *AXIS OS Hardening Guide* should be applied before scanning to avoid false-positives as well as making sure that the Axis device is operated according to Axis cybersecurity recommendations.
- It is recommended to perform a so called credentialed vulnerability scan where e.g. the security scanner is allowed to log in to the Axis device via HTTP(S) or SSH. A credentialed security scan is more effective since the scan surface is widened significantly.
- We emphasize the importance of conducting the vulnerability scan using well-established partners with a broad knowledge and a dedicated set of Axis-specific scanning plugins on the market, such as Tenable, Rapid7, Qualys, or others.

## Most common remarks

### Outdated software components

**Background**
Security scanners highlight when a device is running an outdated version of a software component. It may even occur that the security scanner is unable to determine what version is actually running and flags it anyway. The security scanner simply compares the version of the software components running on the Axis device against the latest available version. The security scanner then outputs a list with security vulnerabilities, even without confirmation that the device being tested is really affected as such. This has been observed with the Linux kernel, OpenSSL, Apache, BusyBox, OpenSSH, cURL and others.

Open-source software components do receive new features, bug fixes and security patches throughout the course of their development, resulting in a high release cycle. Therefore, it is not uncommon that the Axis device being tested is not running the latest version of a software component. However, Axis is monitoring open-source software components for security vulnerabilities that could potentially be deemed critical by Axis, and will publish those accordingly in a *security advisory*.

**Common report terms**

- "A vulnerable version of Linux was found to be utilized"
- "According to its banner, the version of Apache running"
- "According to its banner, the version of OpenSSL running..."
- "Server Version Disclosure (Header)..."

**Risk and recommendations**
From AXIS OS 10.6 and onwards, it's possible to disable the OpenSSL and Apache header information by disabling the parameter **HTTP Server Header Comments** in **Plain config > System**. This may result in vulnerabilities not being detected by security scanners since the package version is not easily identifiable. Axis strongly recommends to keep the AXIS OS on the device up-to-date and encourages to perform security audits on your devices.

### Apache web server

**Background**
Axis devices base their web interface and other web-related functionality on the Apache web server. The web server in Axis devices is primarily being used in two scenarios:

- For general purpose machine-to-machine communication between the Axis device and the system it's connected to, usually a video management system that is accessing the Axis device via API interfaces such as ONVIF and VAPIX.
- The installer, administrators and the end user performing (initial) configuration and maintenance tasks.

The Apache web server is a module-based open-source package. These individual modules can contain vulnerabilities. Below is a list of modules that are commonly loaded and used on Axis devices:

| | | | | |
|---|---|---|---|---|
| core_module (static) | unixd_module (shared) | authn_core_module (shared) | proxy_fcgi_module (shared) | authn_encoded_user_file_module (shared) |
| so_module (static) | alias_module (shared) | authz_core_module (shared) | proxy_http_module (shared) | authz_urlaccess_module (shared) |
| filter_module (static) | rewrite_module (shared) | authn_file_module (shared) | proxy_wstunnel_module (shared) | trax_module (shared) |
| brotli_module (static) | cgid_module (shared) | authz_user_module (shared) | headers_module (shared) | iptos_module (shared) |
| http_module (static) | log_config_module (shared) | authz_owner_module (shared) | http2_module (shared) | axsyslog_module (shared) |

| | | | | |
|---|---|---|---|---|
| suexec_module (static) | setenvif_module (shared) | auth_digest_module (shared) | systemd_module (shared) | ws_module (shared) |
| mime_module (shared) | ssl_module (shared) | auth_basic_module (shared) | authn_axisbasic_module (shared) | |
| mpm_worker_module (shared) | socache_shmcb_module (shared) | proxy_module (shared) | authz_axisgroupfile_module (shared) | |

A vulnerability that applies to a certain module in Apache needs to be loaded and used by the Axis edge device. Vulnerabilities of modules that are not loaded are not relevant.

**Common report terms**

- "Apache HTTPD: mod_proxy_ftp use of uninitialized value (CVE-2020-1934)"

**Risk and recommendations**
Apache vulnerabilities will typically increase risk for public web services exposed to Internet targeting public users. The web server in Axis devices should only be used by installers, administrators and maintainers. It's not recommended to expose Axis devices to be accessible over the Internet, nor should users have privileges to use a web browser to access a device during daily operations. Additional security controls such as IP Tables, only allowing approved clients to access and disabling/preventing web browsers from accessing can be applied to further reduce risks.

## OpenSSL

**Background**
Axis devices use OpenSSL as a common security core component to provide security functionality for, e.g., HTTPS, certificate and encryption use cases. "Outdated OpenSSL version" is a common scanning remark on Axis devices, and new vulnerabilities are discovered frequently in OpenSSL.

Similar to the Apache web server, OpenSSL is a modular-based platform; see below a list of modules that are not utilized by Axis products:

| | | | |
|---|---|---|---|
| no-camellia | no-heartbeats | no-mdc2 | no-srp |
| no-capieng | no-hw | no-rc5 | no-zlibthreads |
| no-dtls | no-idea | no-sctp | |
| no-dtls1 | no-md2 | no-seed | |

A vulnerability that applies to a certain module in OpenSSL needs to be loaded and used by the Axis edge device. Vulnerabilities of modules that are not loaded are not relevant but may still be flagged by the scanning tool.

**Risk and recommendations**
Vulnerabilities in OpenSSL do not pose any risks if the system is not using services such as HTTPS or 802.1x (TLS), SRTP (RTSPS) or SNMPv3. It is not possible to compromise the device itself as a potential attack would target the TLS connections and traffic. Exploiting OpenSSL vulnerabilities requires access to the network, a high skillset and a lot of determination.

## Self-signed certificate

**Background**
Axis devices come with a self-signed certificate that is generated automatically upon first boot in order to provide the possibility to access the product via encrypted HTTPS connection and proceed with the initial setup of the product. Security scanners may highlight the existence of the self-signed certificate as insecure and Axis recommends removing the self-signed certificate from the device and replacing it with a server certificate that is trusted in your organization. The self-signed certificate provides in that sense a confidential and secure mechanism for initial configuration but requires the user to still check the authenticity of the device itself.

**Common report terms**

- "SSL Certificate Cannot Be Trusted..."

- "SSL Self-Signed Certificat"
- "X.509 Certificate Subject CN Does Not Match the Entity Name..."

**Risk and recommendations**
Self-signed certificates provide network encryption but do not protect from man-in-the-middle attacks (a rouge service impersonating a legitimate network service). If using services like HTTPS or 802.x it's recommended to use Certificate Authority (CA) signed certificates. These must be supplied by the system owner using a public or private CA. If not using HTTPS or 802.1x there are no risks, and vulnerabilities in the underlying OpenSSL cannot be used to compromise the Axis device. For Axis devices features Axis Edge Vault, the self-signed certificate was replaced by the IEEE 802.1AR device ID certificate.

## RSA key length

**Background**
As Axis devices come with a pre-loaded self-signed certificate, some devices have a shorter key length for the certificate than the 2048-bits. The certificate is also of a non-standard bit length to ensure most reputable CA's will reject a signing request of this. Security scanners may highlight this as insecure and it is recommended to replace this certificate before production deployment as it is only intended for initial setup.

**Common report terms**

- "SSL Certificate Chain Contains RSA Keys Less Than 2048 bits..."
- "Length of RSA modulus in X.509 certificate: 1536 bits (less than 2048 bits)..."

**Risk and recommendations**
This vulnerability cannot be used to compromise the device. The default self-signed key length of Axis devices is set to 1536 bits in order to reduce the connection latency and time to generate the certificate and key. This key length provides enough protection for administrative tasks such as resetting device account passwords and initial setup of the Axis device. It's recommended to replace the default certificate with a CA-signed certificate that should be provided by the system owner.

## Cipher settings

**Background**
Throughout regular AXIS OS updates, the list of available ciphers of the Axis device may receive updates without the actual cipher configuration being changed. Changing cipher configuration must be user-initiated, either by performing a factory default of the Axis device or via manual user configuration. From AXIS OS 10.8 and onwards, the list of ciphers is automatically updated when the user initiates an AXIS OS update.

**Common report terms**

- "Weak Cryptographic Key..."
- "TLS/SSL Server Supports The Use of Static Key Ciphers..."

It is recommended to always use the strongest ciphers for HTTPS encryption when possible.

TLS 1.2 and lower: When using TLS 1.2 or lower you can specify the HTTPS ciphers to be used in **Plain Config > HTTPS > Ciphers** followed by a restart of the Axis device. Axis recommends to select all or any of the following strong-considered ciphers (updated September 2021), or to do a desired selection of your own.

```
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-
POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
```

TLS 1.3: When using TLS 1.3, the HTTPS ciphers parameter in **Plain Config** has no effect as per default, only strong ciphers according to TLS 1.3 will be selected. The selection cannot be changed by the user and is updated through a AXIS OS update if needed. Currently the ciphers are (updated September 2021):

```
TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_256_GCM_SHA384
```

## Web server remarks

### Boa web server

**Background**

Axis devices with AXIS OS version 5.65 and lower utilize the Boa web server for web interface and web-related functionality. The web server in Axis devices is being primarily used in two scenarios:

- For general purpose machine-to-machine communication between the Axis device and the system it is connected to, usually a video management system that is accessing the Axis device via API interfaces such as ONVIF and VAPIX.
- For configuration and maintenance tasks performed by installers, administrators and end users.

Similar to the newer Apache web server that is utilized by Axis devices with newer AXIS OS, the Boa web server can be affected by vulnerabilities. Security scanners may not recognize the web server used in older Axis devices and will therefore simply assume that these devices utilize the Apache web server. A vulnerability that applies to the Apache web server does not apply to the Boa web server by default if not stated otherwise.

**Common report terms**

- "According to its banner, the version of Apache running..."
- "The version of Apache httpd installed on the remote host is prior to 2.4.46. It is, therefore, affected by multiple vulnerabilities..."

### Apache Struts and Apache Tomcat

**Background**

As described in *Apache web server on page 4* , Axis devices base their web interface and web-related functionality on the open-source Apache web server. Other flavors of the Apache web server exist, such as Apache Struts or Tomcat, but are not utilized in Axis devices. Axis utilizes the plain open-source Apache web server implementation of the Apache Software Foundation (ASF).

**Common report terms**

- "A vulnerability has been discovered in Apache Tomcat..."
- "The Jakarta multipart parser in Apache Struts..."

### Web user sessions

**Background**

Axis devices base their web interface and other web-related functionality on the Apache web server. The web server in Axis devices is primarily being used in two scenarios:

- For general purpose machine-to-machine communication between the Axis device and the system it's connected to, which usually is a video management system that is accessing the Axis device via API interfaces such as ONVIF and VAPIX.
- When the installer, administrators and the end user perform (initial) configuration and maintenance tasks.

During the time a user configures the Axis device using a web browser an attacker may be able to lure the user into accessing a malicious web site or trick them into clicking a disguised link. This is referred as Cross-Site Request Forgery (CSRF). If this occurs while the user has an authenticated session to the device, the attack will re-use the already authenticated web browser session.

Currently, Axis devices do not support traditional web user based sessions where it's possible for the web session to automatically expire after a certain amount of time of user-inactivity while the browser window is open. Every request through the web server on an Axis device has to be authenticated properly in order to be processed before the specific web session is open for further communication. In order to actively close a web session, the browser has to be closed. From AXIS OS 10.12.55 and higher, a logout button has been added to the web interface.

**Common report terms**

## Web server remarks

- "Concurrent User Sessions..."
- "Insufficient Session Termination and Expiry..."
- "Application Lacks Logout Feature..."

**Risk and recommendations**
Axis recommends to access the device through an application, such as a video management system (VMS), as primary video client instead of using the web browser if this would be subject of concerns. However, if the web browser is the only video client available, have the following guidelines in mind:

- Do not to visit untrusted websites or open e-mails from untrusted senders (this is of course a general cyber protection recommendation).
- Use a different browser, which is not the system default, to configure the Axis device.
- Create a viewer account on the device and use this when viewing the video stream. The viewer account has minimal privileges and no rights to change the configuration of the Axis device.
- Do not leave the browser open unattended after configuration in order to minimize the attack window.

Axis also provide *the following statement* that can be used when working with CSRF's in Axis products.

## AXIS OS remarks

### AXIS OS version string

**Background**
Axis discloses vulnerabilities and provides updated AXIS OS with security fixes so that customers can update and mitigate potential risks. Security scanners usually perform only a limited comparison of the AXIS OS version the Axis product is running against older, outdated AXIS OS that may contain vulnerabilities. A security scanner may not recognize the AXIS OS correctly, causing the scanner to flag the AXIS OS running as vulnerable or insecure. Always consult the release notes for the AXIS OS version of the product being tested since serious or critical vulnerability patches are listed in this document.

It may cause confusion if the Axis device is running a custom AXIS OS version or if the security scanner is not updated with the latest information of available Axis AXIS OS. Below are some examples of AXIS OS version strings:

- 9.70 .1
- 9.70 .1_ beta
- 9.70 .1. 5

**Common report terms**

- "Axis Multiple Vulnerabilities (ACV-128401)..."

### Linux distribution and built-in package manager

**Background**
Security scanners may support a so called "credentialed scan" using login data via web-login (HTTP) or via the maintenance access (SSH) in order to get more information about the device, its operating system and other software that might run on it. The Linux distribution is a Poky (OpenEmbedded) version with both local and upstream patches that may not match or can be recognized as such by the security scanner. Furthermore, the security scanner may expect the usage of a package manager, which is not used in Axis products.

Below is a comparison of the naming scheme between the Axis-used distribution and a standard Linux distribution. Note that the latter may be recognized by the security scanner and pass while the Axis version may not. To illustrate this, we have the Axis-specific **4.9.206-axis** and Linux-generic **54.9.206-generic** version strings.

**Common report terms**

- "Local security checks have NOT been enabled because the remote Linux distribution is not supported..."

### Unencrypted AXIS OS and chip

**Background**
Security scanners may highlight the usage of flash chips used in the Axis device and mark them or the filesystems as such with "unencrypted". Axis devices do encrypt user secrets such as passwords, certificates, keys and other files without necessarily encrypting the filesystem. Removable local storage such as SD cards are encrypted using LUKS encryption.

**Common report terms**

- "The flash chip that contains the root file system of the device is not encrypted...."
- "Information was extracted from the unencrypted firmware image, including...."

**Risk and recommendations**
This vulnerability cannot be used to compromise the device. The AXIS OS does not contain any secrets by default and needs no other protection than the AXIS OS signature to validate the integrity. Encrypted software makes it harder for security researchers to identify new (unknown) vulnerabilities, and encrypted software may be used by vendors to hide deliberate flaws (security through obscurity). For Axis devices, root access is required to access the filesystem of the device to gain access to it. Sensitive information such as passwords are stored encrypted on the filesystem and require a high level of sophistication, skillset, time and determination

to extract. Make sure to use a strong root password and keep it protected. Using the same password for multiple cameras simplifies management but increases the risk if one camera's security being compromised.

## Bootloader

**Background**
Security scanners may believe that they have identified the make and model of the bootloader implementation used in Axis devices and could therefore highlight vulnerabilities related to secure boot or the bootloader itself. Axis network video and network audio products utilize an in-house developed bootloader referred to as nandboot/netboot.

**Common report terms**

- "A vulnerability in all versions of the GRUB2 bootloader has been detected..."
- "An issue was discovered in Das U-Boot through 2019.07..."

## Network remarks

### TCP/ICMP timestamp response

**Background**
While TCP and ICMP timestamp information is most often used as network tools to measure performance and availability of hosts, it can also be used to find time-related information about the network device itself. The ICMP timestamp information in ICMP type 13 (timestamp request) and ICMP type 14 (timestamp reply) communication provides information that could be used to calculate the actual device time in UTC. The TCP timestamp information can be used to calculate the so called round-trip time (RTT) information between two network hosts, which would make it possible to calculate the current uptime of the Axis device.

Security scanners may flag the existence of TCP and ICMP timestamp responses from Axis devices and recommend to disable TCP and ICMP timestamp responses whenever possible. Axis follows the recommendation of the Linux open-source community which does not consider the actual date/time information provided from these responses as a security risk by itself. Therefore the TCP/ICMP timestamp responses are still enabled by default. Furthermore, in newer Linux Kernel versions the actual calculation is considered unreliable as counter-measures ensure to make it unreliable to calculate the date/time information. As of today (February 2022), no known vulnerabilities or exploits have been disclosed that would justify disabling these services in Axis devices.

**Common report terms**

- "TCP timestamp response found..."
- "ICMP timestamp response found..."

### HTTP(S), HSTS policy

**Background**
Axis devices are configured by default to allow HTTP and HTTPS connections. It is recommended to make use of the first-boot generated self-signed certificate in order to perform the first initial configuration of the Axis device in HTTPS mode and to switch the configuration to only allow for HTTPS connections. HTTPS can be enforced e.g. from the web interface of the Axis device following **Settings > System > Security**. Furthermore, using HSTS (HTTP Strict Transport Security) to further increase device security is automatically enabled only when the Axis device is operated in HTTPS-only mode. HSTS is supported in the 2018 LTS (8.40), 2020 LTS (9.80) and the AXIS OS 10.1 active track.

Security scanners may highlight that the Axis device being tested is configured to allow HTTP only or HTTP & HTTPS at the same time. The detection is usually performed by validating the response from and checking the port status of the standard HTTP port 80. Axis recommends to use the device in HTTPS mode only by configuring this accordingly. Many security scanner audits are performed on Axis devices where this specific HTTPS-only configuration is not enforced by allowing the Axis device to respond to HTTP and/or HTTPS connections.

**Common report terms**

- "HTTP (Port 80) insecure channel detected..."
- "Web Portal Allows Unencrypted HTTP Connections By Default..."
- "The remote web server is not enforcing HSTS, as defined by RFC 6797..."
- "Insufficient Transport Layer Security..."

### Echo Service Detection

**Background**

The Echo service can be spoofed into sending data from one service on one device to another service on another device. This action causes an infinite loop and creates a denial of service attack. The attack can consume increasing amounts of network bandwidth, causing loss of performance or a total shutdown of the affected network segments.

Axis devices are configured by default to not utilize the Echo service nor are listening to port 7 (TCP/UDP) used by the Echo service.

## Network remarks

**Common report terms**

- “Echo Service Detection...”
- "Echo command detected...”
- "Echo service running...”

## Hardware remarks

### Architecture vulnerabilities

**Background**
Certain vulnerabilities may depend on the processor architecture that a device is using. Axis edge devices, such as cameras, encoders, wearables, audio and intercom products, are based on MIPS and ARM architecture and are, e.g., not affected by x64 or x86 architecture-based vulnerabilities.

**Common report terms**

- "OpenSSL rsaz_512_sqr overflow bug on x86_64 (CVE-2019-1551)..."
- "x64_64 Montgomery squaring procedure..."

### UART / Serial console

**Background**
Every Axis device incorporates a so called physical UART (Universal Asynchronous Receiver Transmitter) interface, sometimes referred to as a debug port or serial console. The interface itself is not easily accessible. To gain physical access, extensive dismantling of the Axis device is required. The UART/debug interface is used only for product development and debugging purposes during internal R&D engineering projects within Axis.

For Axis devices with AXIS OS 10.10 and lower, the UART/debug interface is enabled by default, but it requires authenticated access and does not expose any sensitive information while being unauthenticated. From AXIS OS 10.11 and onwards, the UART/debug interface is disabled by default and can only be enabled by unlocking it via a device-unique custom certificate. This is provided by Axis only and cannot be generated in any other way.

**Common report terms**

- "Information Disclosure via UART/Serial Console..."
- "Root Shell via UART/Serial Console..."
- "On the PCB, the headers exposed a UART console..."

Ver. M10.2

AXIS OS Vulnerability Scanner Guide

Date: October 2022

Part no.