Technical note

Common remarks from security scanner tools

AXIS COMMUNICATIONS

Table of contents

1. About this document

The purpose of this document is to assist device owners to interpret results from vulnerability scanning tools in order to make a risk assessment.

2. 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. The Axis Hardening Guide describes several security controls and recommendations how to minimize risks when deploying, operating and maintain an Axis device.

Some vulnerabilities may be easy to exploit, 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 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 that publish 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 remediated in future firmware releases. Vulnerabilities that Axis identifies as increased risk will be treated with priority resulting in an unscheduled firmware patch or publishing of a Security Advisory, informing about the risk and recommendations.

3. Scanning tools reporting false-positive

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 firmware version as it may include patches that address several vulnerabilities.

4. Boa web server

Background
Axis devices with firmware 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 firmware, the Boa web server can be affected by vulnerabilities.

Motivation for false-positives
Security scanners may not recognize the web server used in older Axis devices and will therefore simply assume that those 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..."

5. 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 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.

> 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 modules individually can contain vulnerabilities.

Below is a list of modules that are commonly loaded and used on Axis devices:

core_module (static)
so_module (static)
filter_module (static)
brotli_module (static)
http_module (static)
suexec_module (static)
mime_module (shared)
mpm_worker_module (shared)
unixd_module (shared)
alias_module (shared)
rewrite_module (shared)
cgid_module (shared)
log_config_module (shared)
setenvif_module (shared)
ssl_module (shared)
socache_shmcb_module (shared)
authn_core_module (shared)
authz_core_module (shared)
authn_file_module (shared)
authz_user_module (shared)
authz_owner_module (shared)
auth_digest_module (shared)
auth_basic_module (shared)
proxy_module (shared)
proxy_fcgi_module (shared)
proxy_http_module (shared)
proxy_wstunnel_module (shared)
headers_module (shared)
http2_module (shared)
systemd_module (shared)
authn_axisbasic_module (shared)
authz_axisgroupfile_module (shared)
authn_encoded_user_file_module (shared)
authz_urlaccess_module (shared)
trax_module (shared)
iptos_module (shared)
axsyslog_module (shared)
ws_module (shared)

Motivation for false-positives
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 is 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.

6. Apache Struts and Tomcat

Background
As described earlier in section 4. Apache web server, Axis devices base their web-interface and web-related functionality on the open-source Apache web server. Other flavours of the Apache web server exist, such as Apache Struts or Tomcat but are not utilized in Axis devices.

Motivation for false-positives
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...".

7. OpenSSL

Background
"Outdated OpenSSL version" is a common scanning remark on Axis devices. New vulnerabilities are discovered frequently in OpenSSL. Axis devices use OpenSSL as a common security core component in its products which provide security functionality for, e.g., HTTPS, certificate and encryption use cases. 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-capieng
no-dtls
no-dtls1
no-heartbeats
no-hw
no-idea
no-md2
no-mdc2
no-rc5
no-sctp
no-seed
no-srp
no-zlib
threads

Motivation for false-positive
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.

8. First-boot generated 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.

Motivation for false-positives
Security scanners might 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 check still the authenticity of the device itself.

Common report terms
"SSL Certificate Cannot Be Trusted"
"SSL Self-Signed Certificate"
"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 is 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.

9. 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.

Motivation for false-positive
Security scanners may highlight this as insecure. 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 is recommended to replace the default certificate with a CA-signed certificate that should be provided by the system owner.

10. 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.

Motivation for false-positives
Below is a comparison between a standard Linux distribution and the Axis-used distribution when it comes to the naming scheme. Please note that the latter may be recognized by the security scanner and pass while the Axis version may not pass.

4.9.206-axis5
4.9.206-generic

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

11. Axis firmware version string

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

Motivation for false-positives
This may can cause confusion in case the Axis device is running a custom firmware version or if the security scanner is not updated with the latest information of available Axis firmware.

9.70.1
9.70.1_beta
9.70.1.5

Common report terms
"Axis Multiple Vulnerabilities (ACV-128401)"

12. Architecture-dependent vulnerabilities

Background
Certain vulnerabilities may depend on the processor architecture that a device is using.

Motivation for false-positives
Axis devices 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"

13. 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, so flags it anyway. The security scanner simply compares the version of those 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 under test is really affected as such.

The above has been observed with the Linux kernel, OpenSSL, Apache, BusyBox, OpenSSH, Curl and others.

Motivation for false-positives
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 under test 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 on: www.axis.com/support/product-security.

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..."

14. Unencrypted firmware/chip

Background
Security scanners may highlight highlight the usage of flash chips that are used in the Axis device and mark them or the filesystems as such with "unencrypted".

Motivation for false-positives
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 firmware does not contain any secrets by default and needs no other protection than the firmware 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 delibrate 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 is compromised.

15. Bootloader

Background
Security scanners may believe that they have identified the make and model of the bootloader implementation Axis is using in their products and therefore highlight vulnerabilities with regards to secure boot or the bootloader itself.

Motivation for false-positives
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...".

EN/R1/2012

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, Axis offers products and services for video surveillance and analytics, access control, intercom and audio systems. Axis has more than 3,800 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.