CYBERSECURITY

Device lifecycle management

Cybersecurity risks exist at every step of a networked device's lifecycle, from production to decommissioning. If these risks are overlooked, they can lead to operational disruptions, and loss of confidentiality, integrity and availability of data. So it's crucial that all stakeholders, from the supplier to the end customer, take the responsibility to manage risks.

Considerations for the device security lifecycle are, therefore, important in procurement. A manufacturer should have measures to reduce cybersecurity risks before the product reaches the customer, while the product is in service, and when the product is decommissioned.

The following pages provide a glance at the technologies, tools and guidance, as well as the approaches and processes that Axis supports to mitigate risks throughout the lifecycle of an Axis device.

Security foundation: Axis Edge Vault, AXIS OS, Axis Security Development Model

Security foundation – hardware, software and approach

Protecting product integrity and reducing the risk of vulnerabilities right from the start

Axis Edge Vault cybersecurity platform
This hardware-based platform includes features that safeguard the device's identity and integrity, so you can securely boot the device, integrate it and ensure sensitive data, like cryptographic keys, are protected from unauthorized access.

Operating system, AXIS OS
AXIS OS drives a range of Axis devices. Incorporating industry best practices in vulnerability management, AXIS OS provides the platform to quickly and efficiently release software security features and patches across a great number of products.

Axis Security Development Model (ASDM)
It's a methodology applied at Axis to reduce the risk of releasing products with software vulnerabilities. ASDM ensures that security considerations are an integral part of software development and involves, among other things, risk assessments, threat-modelling, analysis of code, penetration testing, bug bounty program, and vulnerability scanning and management.

Transparency
It's an important part of Axis' way of working to build trust. Axis is a Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA). We publish and notify stakeholders about vulnerabilities so customers can take appropriate action. We also publish a software bill of materials (SBOM) and end-of-support date for a device's operating system (AXIS OS).

PRODUCTION AND DISTRIBUTION

Reducing the risk of compromised components

- **Supply chain:** Critical components are procured directly from strategic suppliers. Axis works closely with manufacturing partners. Production processes are monitored, and data is shared 24/7 with Axis, enabling real-time analysis and transparency.
- **Axis Edge Vault:** Installed on an Axis device during production, Axis Edge Vault includes the following features:
  - **Secure keystore,** which involves cryptographic computing modules (like secure element, Trusted Platform Module, Trusted Execution Environment) for storage of cryptographic keys.
  - **Signed firmware,** which guarantees that the installed AXIS OS is genuinely from Axis. It ensures that any new firmware to be downloaded and installed on the device is also signed by Axis.
  - **Secure boot,** which enables the device to check that the firmware has an Axis signature. If the firmware is unauthorized or has been altered, the boot process is aborted and the device stops running. The combination of signed firmware, secure boot and making a factory default on the device offers protection from malicious modifications during the shipment of a device.
  - **Axis device ID**, which is a device-unique certificate with corresponding keys that can prove the authenticity of an Axis device. The device ID, which is IEEE 802.1AR-compliant, enables secure device identification and onboarding on a network.
  - An **encrypted file system**, which protects customer-specific configuration and information stored in the file system from being extracted or tampered with while the device is not in use, such as when it is in transit from a system integrator to the end customer.

IMPLEMENTATION

Addressing the risks of putting compromised or inadequately hardened products on the network that may lead to unauthorized access, extraction of sensitive data, and altered data being transferred between network endpoints

- **Factory default:** Perform a factory default on the device prior to configuring it. This guarantees that the device is completely free of unwanted software or configuration since the only software remaining is AXIS OS and its default settings.
- **Check for the latest firmware or AXIS OS version for the device:** Some time may have passed between production and implementation, so it's a good idea to check on the Axis website for the latest AXIS OS version, which may contain the latest bug fixes for the particular device.
- **Axis device ID:** To ensure only genuine Axis devices are implemented on the network, the Axis device ID can be verified using IEEE 802.1X authentication or when establishing a secure network connection through the HTTPS protocol. On an IEEE 802.1X network, the Axis device ID can be leveraged to increase security and decrease deployment time.
- **Secure keystore:** Involving cryptographic computing modules, secure keystore holds sensitive information like the Axis device ID and customer-loaded keys, preventing unauthorized access and malicious extraction of sensitive information, even in the event the device is compromised.
- **Encrypted file system:** This ensures no data stored in the file system can be extracted or tampered with when the device is not in use.
- **Hardening guides:** The AXIS OS Hardening Guide, available on the AXIS OS portal on the Axis website, establishes a baseline configuration to address common threats, providing best practices and technical advice. There is also a hardening guide for the video management software, AXIS Camera Station, as well as for Axis network switches.
- **AXIS OS Security Scanner Guide:** Axis recommends running security scans of Axis devices to see if they are affected by vulnerabilities or weak configuration. The AXIS OS Security Scanner Guide offers recommendations on how to solve certain remarks from the scanners and outlines the common "false positives".
- **AXIS Device Manager:** This tool provides for efficient configuration and management of Axis devices locally. It enables batch processing of installation and security tasks, such as managing device credentials, deploying certificates, disabling unused services, and upgrading AXIS OS.


PRODUCTION


DISTRIBUTION


IMPLEMENTATION


IN SERVICE


DECOMMISSIONING

IN SERVICE

Addressing risks from running firmware with known vulnerabilities, updating devices with unauthenticated firmware, or letting secure configurations lapse

> **Upgrade firmware/operating system:** It is essential to maintain the cybersecurity of an Axis device by keeping the firmware up to date using either the AXIS OS active track or the long-term support (LTS) track. Provided free of charge, firmware updates using either track will include security patches. Signed firmware ensures only genuine AXIS OS can be installed.

> **AXIS Device Manager Extend:** This tool, which complements the AXIS Device Manager, allows for remote management of Axis devices and simplifies scaling of maintenance tasks, such as upgrading a device's firmware.

> **Vulnerability management:** Axis provides a security notification service that you can sign up to for information about vulnerabilities and other security-related matters.

> **AXIS OS Forensic Guide:** The guide provides technical advice for anyone conducting forensic analysis of Axis devices in the event of a cybersecurity attack on the surrounding network and IT infrastructure where an Axis device is installed.

> **Signed video:** When this feature is enabled in a supported camera, cryptographic signatures are added to the video stream before it leaves the device, enabling viewers to verify if the video has been tampered with or not. This is particularly important in an investigation or prosecution.

DECOMMISSIONING

Addressing the risk of devices that are no longer supported and have known, unpatched vulnerabilities, as well as the risk of sensitive data left on devices after disposal

> **Firmware end-of-support date:** The support web page for many products on Axis.com shows the end-of-support date for the particular product's operating system, enabling customers to plan for the decommissioning and replacement of the product in a timely manner.

> **AXIS Device Manager Extend:** It provides for easy tracking of the warranty status for all devices in the system, including product discontinuation and end of support information. This information allows you to prepare a device for decommissioning and eliminate the risk that an unsupported device presents.

> **Guidance:** The AXIS OS portal on the Axis website provides guidance on decommissioning an Axis device. Making a factory default on a device erases all configurations and data.

For more information, please visit: **www.axis.com/cybersecurity**