

Keine Angst vor NIS2 mit Axis Geräten

Axis Communications | Christian Schilffarth

Über mich ...

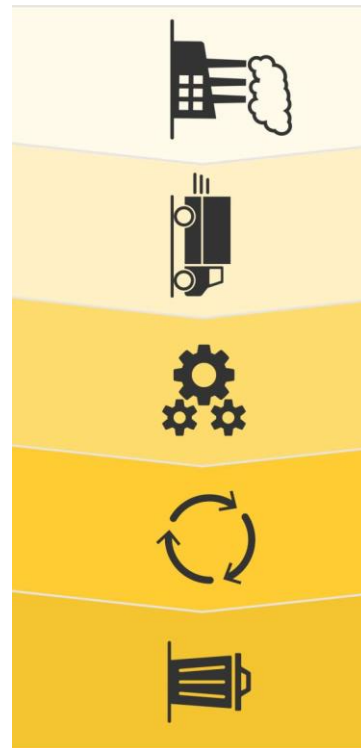
- > **Christian Schilffarth**
- > Technischer Trainer & Consultant
- > 9 Jahren Axis Communications
- > Themenschwerpunkte:
 - ameratechnik
 - Netzwerktechnik
 - Videomanagement
 - Cybersecurity (IT-Sicherheit)



christian.schilffarth@axis.com

Axis Security by Design – Life Cycle Management

- > Entwicklung und Produktion
 - Axis Security Development Model
 - Sicherer Zertifikats-/Schlüsselspeicher
 - ARTPEC Chip: Designed by Axis
- > Lagerung und Auslieferung
 - Gatekeeper Funktion
- > Wartung und Pflege
 - Axis Device Manager
 - CVE Report
 - Firmware Updates (LTS/Active Track)
- > End of Life / End of Service
- > Außerbetriebnahme



Axis Security by Design – Hardening Guide



Access control

Access control management

Local user device management with password complexity indicator
Federated user device management through OpenID Connect (RFC6749, 1.3.1 Authorization Code) providing ADFS-integration that unlocks features such as Password complexity enforcement, rotation, automatic account lock-out Multi-factor authentication (MFA), Microsoft AD entitlement functionality



Privacy

Use of diagnostics data
Minimalistic approach to how much customer-specific should be stored



Application

Application security

TLS-based application security (MQTT, SFTP, NTS, HTTPS, WebRTC)
Encrypted video streaming (RTSPS/SRTP, HTTPS), Secure remote syslog



Operating system

Encryption and data protection

OpenSSL 1.1.1 and 3.0
X.509 certificate PKI and cryptography
Transport layer security (TLS 1.2/TLS 1.3)
SD card encryption (AES-XTS-Plain64 256bit)
Encrypted file system (AES-XTS-Plain64 256bit),
Signed video



Default security

HTTPS enabled by default
Brute-Force Delay Protection
Host-based Firewall
Network time security (NTS)
Insecure TLS versions disabled
UART/Debug port disabled



Enterprise network security

IEEE 802.1X (network access control)
IEEE 802.1AR (secure device identity)
IEEE 802.1AE (MAC security, MACsec)



AXIS OS Operating System

Common Linux-based operating system with more than 95% industry-standard open-source software components such as OpenSSL, Apache, Curl and others.
Active track for feature growth and 5-Year Long-Term Support tracks (LTS) for 3rd party integration and backwards-compatibility use cases.



Silicon assisted security (chip)

Hardware root-of-trust

ARM-based system-on-chip (SoC) security
Trusted Execution Environment (TEE/OP-TEE)
Trusted platform module (TPM 2.0), Secure element



Secure key storage

Tamper-protected storage and operation of cryptographic keys such as customer uploaded private keys, video signing keys and the Axis Device ID.



Security foundation

Secure software development

Axis security development model (ASDM)
3rd party penetration tests
Bug bounty program with Bugcrowd
Software Bill of Material (SBOM)



Certification

Common criteria CC EAL4+ / EAL6+
FIPS 140-2
ETSI EN 303 645



Trusted device identity

Axis Edge Vault cybersecurity platform
Secure boot with Signed Firmware (code-signing)
Axis Device ID (IEEE 802.1AR)



Axis Security by Design – Vulnerability Management

- > Axis Bug Bounty Programm
- > Cybersecurity Newsletter
- > Anleitung zum sicheren Betrieb
- > CVE-Reports direkt von Axis

List of outstanding contributors

Axis would like to thank the following independent researchers and companies for their contribution in securing Axis products, software and services. We appreciate your hard work and dedication.

2023

- [Alexander Pick](#) - [CVE-2023-21404](#)
- [Domain Chaser](#)

2022

- Genetec Inc. - Security Team
- SeungYun Lee - [CVE-2022-23410](#)
- [James Tsz Ko Yeung](#) - [CVE-2022-23410](#)
- Gaurang Maheta

2021

- [Andrea Palanca](#) - [CVE-2021-31988](#)
- Ben Leonard-Lagarde - [CVE-2021-31988](#)
- [Freddie Sibley-Calder](#) - [CVE-2021-31988](#)

Axis lists all researchers who contributed to the CVE program. Axis became a CVE Numbering Authority (CNA) in 2021.

Security Advisory

CVE-2023-21404 - 08.05.2023 (v1.0)



Affected products, solutions, and services

- AXIS OS 11.0.X - 11.3.x

Summary

Alexander Pick, member of the [AXIS OS Bug Bounty Program](#), has found a flaw that does not follow Axis secure development best practices. A static RSA key was used to encrypt Axis-specific source code in legacy LUA-components. The encryption was applied to avoid non sensitive Axis-specific code from being easily human readable. The encryption using a static RSA key is not necessary since it is neither protecting sensitive data, nor can it be used to compromise Axis devices or customer data.

The vulnerability has been assigned a [4.1 \(Medium\)](#) severity by using the CVSSv3.1 scoring system. Learn more about the Common Vulnerability Scoring System [here](#).

Solution & Mitigation

Axis has released a patched version of AXIS OS (version 11.4.52) that removes the LUA-component. No patch will be made available for the long-term support (LTS) tracks as the LUA-components cannot be removed due to backwards compatibility reasons. Since the static RSA key is not protecting sensitive data, a non-patched AXIS OS version does not imply any practical risk.

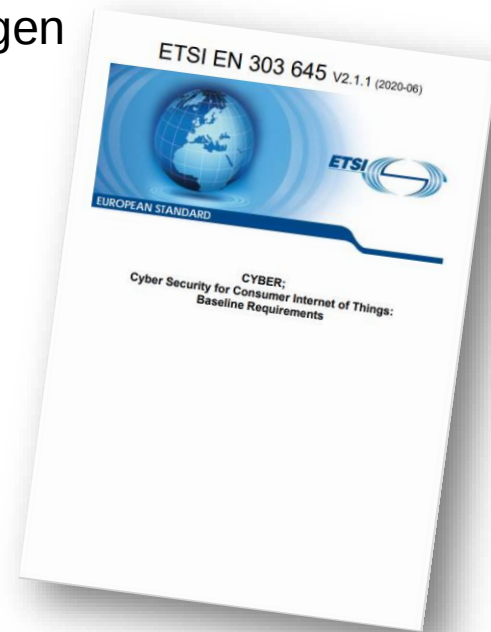
The release notes will state the following:

Corrected CVE-2023-21404. For more information, please visit the [Axis vulnerability management portal](#).

The latest AXIS OS can be found [here](#). For further assistance and questions, please contact [AXIS Technical Support](#).

Cybersicherheit - Security and Privacy by Design

- > **ETSI EN 303 645** definiert Basissicherheitsanforderungen an IoT-Geräte
 - Beinhaltet 68 technische Anforderungen, die die Cybersicherheit eines IoT's sicherstellen sollen
- > Axis Produkte, die mit AXIS OS 11 oder höher laufen, haben eine Zertifizierung für die Einhaltung der ETSI EN 303 645 erhalten



Konkrete technische Maßnahmen

Sicher Plattform – Axis ARTPEC

- > Axis Chip-Satz (kein OEM/ODM)
- > Leistungsstarke Plattform
- > Zentrale Einheit in allen Axis-Geräten
 - Bildverarbeitung
 - Datenkommunikation
 - Systemsicherheit



Axis sichere Inbetriebnahme

- > Alle Funktionen deaktiviert
 - Reduziert auf Geräte GUI
- > Kein Standard-Benutzer
 - Sichere Konto muss angelegt werden
- > Aktivieren der Sicherheit
 - Zero-Trust-Prinzip
 - Mit *AXIS Camera Station* (VMS) automatisiert
 - Zusätzliche Netzwerksicherheit



Axis OS Strategie

Active Track

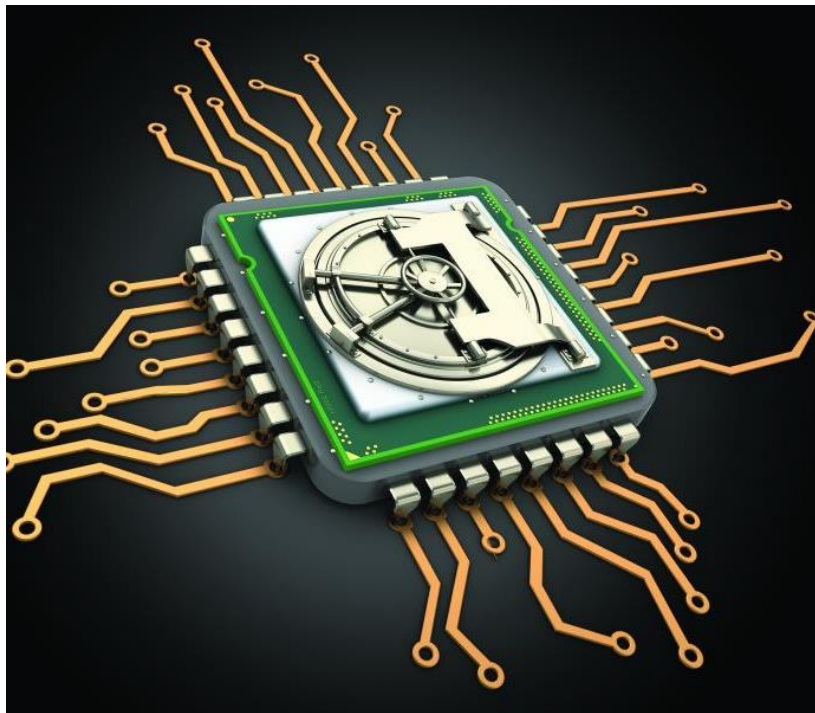
- Neue Funktionen
- AXIS End to End Solutions
- Neue Produkte
- Support-Voraussetzung

LTS Track

- System Kompatibilität
- 3rd party VMS & Anwendungen
- Maximale Stabilität
- 5+ Jahre Support

Bugfixes & Security-Verbesserungen

Axis OS Cyber-Sicherheit



- > Signed Firmware
 - Daten-Integrität beim FTP-Download
- > Secure Boot
 - Integrität des Flash-ROM und der Anwendungen
- > Signed Video
 - Digitale Signatur des Video-Streams
 - Sichert Unveränderbarkeit
 - Zeigt Videodatenquelle
 - Unterstützt von *Axis File Player*

Sicherer Schlüsselspeicher

- > Axis Edge Vault
 - Bei der Geräteproduktion hinzugefügt
 - Nicht löschbar/austauschbar/ manipulierbar
 - Vielfältig einsetzbar
 - Vertrauenswürdiges Axis Referenzzertifikat
- > Trusted Platform Module (TPM)
 - Hardware basierte Funktion
 - FIPS 140-2 Zertifiziert (US by NIST)
 - Zertifiziert für Sicherheitsstufe 2
 - In Ausgewählten Axis Geräte integriert



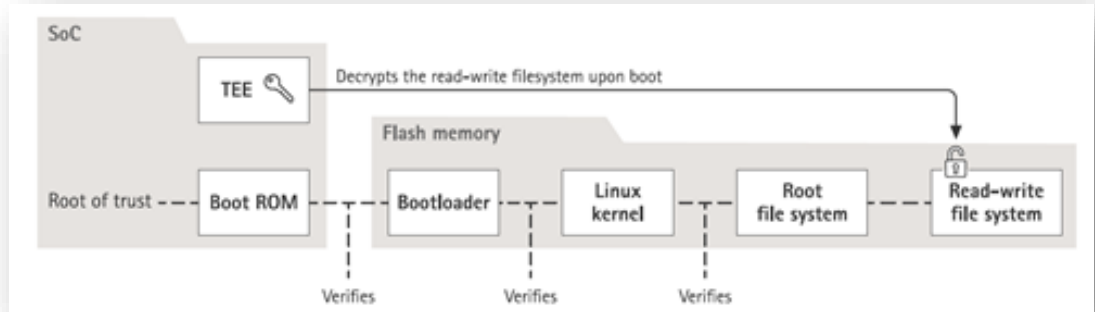
Sichere Verbindung im Netzwerk

- > Netzwerksicherheit
 - IEEE 802.1 X (der Klassiker)
 - IEEE 802.1 AE (Axis Device ID)
 - IEEE 802.1 AR (MACsec)
- > Ende-zu-Ende-Verschlüsselung
 - HTTPS (mit TLS)
- > Sichere Videoübertragung
 - RTSPS (Videostream verschlüsselt)
 - Signiertes Video



Das geschützte Dateisystem

- > Schutz der sensiblen Daten
- > SoC: System on Chip
- > Trusted Execution Environment (TEE)
- > Verschlüsselt, wenn ausgeschaltet
- > Standardfunktion aktiv



Werkzeugkasten – AXIS Device Manager

- > Inbetriebnahme
 - Verwalterkonto anlegen
 - Sicherheitsfunktionen anpassen
 - Netzwerkkonfiguration
 - Zugriff auf Geräte GUI
- > Wartung und Pflege
 - EoL und EoS Info
 - Axis OS Update
 - Gerätekonfiguration
- > Gerätesicherheit
 - Benutzerverwaltung
 - Root CA für TLS
 - Zertifikatsverteiler für IEEE802.1X
- > ACAP-Verwaltung
 - Installation & Konfiguration
 - Registrierung & Lizenzierung
- > Werkzeuge für das „Troubleshooting“

