NCC Group
650 California St, Suite 2950
San Francisco, CA 94108
https://nccgroup.com

August 3, 2023

Axis Communications AB
Gränden 1
SE-223 69 Lund

Introduction

Between the days of July 10th and July 21st, 2023, two (2) consultants from NCC Group engaged in testing the Axis Secure Boot implementation for a total of sixteen (16) person-days of effort, reviewing the Axis ARTPEC-8 bootloader. Reference product under test was a AXIS M3215-LVE Dome Camera and operating system version AXIS OS 11.5.

The purpose of this assessment was to identify application-level security issues that could adversely affect the security of the ARTPEC-8 Bootloader application. This assessment was performed by NCC Group under the guidelines provided in the statement of work for the engagement.

Detailed Letter of Engagement Overview

NCC Group is a global information assurance firm that, in the US, specializes in application, mobile, network, host, and product security. Security conscious companies use NCC Group's Detailed Letters of Engagement to verify product attributes in view of current security best practices, standard security functionality, and product protection. More information about the Group's processes and products can be found at https://nccgroup.com/us.

It is important to note that this document represents a point-in-time evaluation of security posture. Security threats and attacker techniques evolve rapidly, and the results of this assessment are not intended to represent an endorsement of the adequacy of current security measures against future threats. This Detailed Letter of Engagement necessarily contains information in summary form and is therefore intended for general guidance only; it is not intended as a substitute for detailed research or the exercise of professional judgment. The information presented here should not be construed as professional advice or service.

Testing Methods

Testing was performed using NCC Group's standard methodology for a white box security assessment. Axis Communications AB provided NCC Group with access to source code and documentation in order to improve the effectiveness of the testing. The following aspects of the ARTPEC-8 Bootloader were reviewed as part of this assessment:

- Ensure that Axis has implemented all industry standard bootloader security functions
- Validate that each step in the boot chain is correctly verifying the cryptographic signature of subsequent code modules
- Ensure that the boot code is free of common firmware image or metadata parsing vulnerabilities that could lead to a Secure Boot bypass
- Assess any install-time firmware validity tests for similar classes of vulnerabilities
- Verify flash partition signing and whether tampering with partition contents by means of a simple chip-off attack may allow an attacker to tamper with critical kernel/boot parameters

- Review interaction of bootloader with external flash memory in order to observe race conditions such as double-fetch or time-of- check-time-of-use
- Assess the storage of sensitive cryptographic assets used for boot chain verification, in volatile and non-volatile memory
- Enumeration of any unauthenticated bootloader interfaces intended for software loading, manufacturing, repair, or debugging
- Inspect the hardware design (schematic and SoC configuration) to ensure that all relevant security functions are enabled correctly and that it is free of programmatic security bypass features such as strap resistors, jumpers, or other optional functionality

Bootloader trustzone services assessment

- Review key and secret management
- Assess the correct dropping of privileges as the system moves from secure mode to the non-secure mode
- Review the loading routines that parse, validate, and run the main trustzone runtime firmware image (itself out of scope)

Summary of Findings

The main execution path correctly validated signatures, and associated metadata where required. Nevertheless, other code paths such as Ethernet boot, error handling and dormant PCIe functionality were not as robust and contained vulnerabilities that may allow an attacker to bypass the security guarantees of the secure boot implementation. As is typical with secure boot bypass vulnerabilities, physical access may be required to exploit them.

During the assessment, NCC Group identified:

- One (1) high severity vulnerability **[1]**
- One (1) medium severity vulnerability**[2]**
- One (1) low severity vulnerabilities **[3]**
- Three (4) informational findings

Upon completion of the assessment, all findings were reported to Axis Communication AB along with recommendations.

Statement from Axis Communications AB

[1] *Patched in AXIS OS 11.6 (September 2023), CVE-2023-21414*
[2] *General remark to be considered in future development of Secure Boot to increase robustness against sophisticated physical attacks*
[3] *Patched in AXIS OS 11.8 (January 2024)*