Security Advisory

CVE-2023-21414 - 16.10.2023 (v1.0)

Affected products, solutions, and services

- Axis ARTPEC 8 products running AXIS OS 10.11 - 11.5
- AXIS A8207-VE Mk II < AXIS OS 11.5
- AXIS Q3527-LVE AXIS OS 10.11 - AXIS OS 11.5

Summary

NCC Group has found a flaw during the annual penetration test ordered on behalf of Axis Communications. The protection for device tampering (commonly known as Secure Boot) in AXIS OS was vulnerable to a sophisticated attack to bypass this protection. To Axis' knowledge, no known exploits exist publicly as of today and Axis is not aware that this has been exploited.

The vulnerability has been assigned a 7.1 (High) 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 for affected AXIS OS versions on the following tracks:

- Active Track 11.6.94
- LTS 2022 10.12.206

The release notes will state the following:
Corrected CVE-2023-21414. Affected products are AXIS A8207-VE Mk II, AXIS Q3527-LVE and all ARTPEC 8 products. Note that downgrading the product to an older AXIS OS version other than the latest supported 10.12 LTS track release is not possible except for AXIS Q3527-LVE that has support for 9.80 LTS. For more information, please visit the Axis vulnerability management portal.

It is recommended to update the Axis device software. The latest Axis device software can be found here. For further assistance and questions, please contact Axis Technical Support.

Axis Communications AB, Gränden 1, SE-223 69 Lund, Sweden
Tel: +46 46 272 18 00, Fax: +46 46 13 61 30, www.axis.com