Security Advisory

CVE-2024-6979 - 10.09.2024 (v1.0)

Affected products, solutions, and services

- AXIS OS 11.11

Summary

Amin Aliakbari, member of the AXIS OS Bug Bounty Program, has found a broken access control which would lead to less-privileged operator- and/or viewer accounts having more privileges than designed. The risk of exploitation is very low as it requires complex steps to execute, including knowing of account passwords and social engineering attacks in tricking the administrator to perform specific configurations on operator- and/or viewer-privileged accounts.

For security reasons, Axis will not provide more detailed information about the vulnerability. Axis appreciates the efforts of security researchers and ethical hackers on improving security in Axis products, solutions, and services.

The vulnerability has been assigned a 6.8 (Medium) severity by using the CVSSv3.1 scoring system. Learn more about the Common Vulnerability Scoring System here.

Solution & Mitigation

Axis has released a patch for the affected AXIS OS version on the following track:

- LTS 2024 11.11.94

The release notes will state the following:
Addressed CVE-2024-6979. For more information, please visit the Axis vulnerability management portal.

Axis devices not included in these tracks and still under support will receive a patch according to their planned maintenance and release schedule.

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