Security Advisory

CVE-2024-0067 - 10.09.2024 (v1.0)

Affected products, solutions, and services

- AXIS OS 8.40 – AXIS OS 11.10

Summary

Marinus Pfund, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API *ledlimit.cgi* was vulnerable for path traversal attacks allowing to list folder/file names on the local file system of the Axis device. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. 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 4.3 (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 affected AXIS OS versions on the following tracks:

- LTS 2024 11.11.73
- LTS 2022 10.12.249
- LTS 2020 9.80.78
- (Former LTS) 8.40.59 for products that are still under AXIS OS software support.

The release notes will state the following:
Addressed CVE-2024-0067. 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.