

Security Advisory



CVE-2024-47260 - 04.03.2025 (v1.0)

Affected products, solutions, and services

- AXIS OS 9.80 - 12.2

Summary

5113nc3, member of the [AXIS OS Bug Bounty Program](#), has found that the VAPIX API `mediaclip.cgi` did not have a sufficient input validation allowing for uploading more audio clips than designed resulting in the Axis device running out of memory. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account.

To Axis' knowledge, no known exploits exist publicly as of today and Axis is not aware that this has been exploited. Axis will not provide more detailed information about the vulnerability. We appreciate the efforts of security researchers and ethical hackers on improving security in Axis products, solutions, and services.

The vulnerability has been assigned a [6.5 \(Medium\)](#) severity by using the CVSSv3.1 scoring system. [CWE-641: Improper Restriction of Names for Files and Other Resources](#) has been assigned by using the CWE mapping. Learn more about the Common Vulnerability Scoring System and the Common Weakness Enumeration mapping [here](#) and [here](#).

Solution & Mitigation

Axis has released a patch for this flaw with the following versions:

- Active Track 12.3.1
- LTS 2024 11.11.135
- LTS 2022 10.12.270
- LTS 2020 9.80.89

The release notes will state the following:

Addressed CVE-2024-47260. For more information, please visit the [Axis vulnerability management portal](#).

Due to the low impact of this CVE, an out-of-band release will not be provided. A patch will be provided with [the next planned release](#) when available. 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](#).