

Security Advisory

CVE-2023-21415 - 16.10.2023 (v1.1)



Affected products, solutions, and services

- AXIS OS 6.50 – AXIS OS 11.5

Summary

Sandro Poppi, member of the [AXIS OS Bug Bounty Program](#), has found that the VAPIX API `overlay_del.cgi` was vulnerable to path traversal attacks that allows for file deletion. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. The impact of exploiting this vulnerability is lower with operator service accounts and limited to non-system files compared to administrator-privileges. 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 [6.5 \(Medium\)](#) 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
- LTS 2020 9.80.47
- LTS 2018 8.40.35
- (Former LTS) 6.50.5.14 for products that are still under AXIS OS software support.

The release notes will state the following:

Corrected CVE-2023-21415. 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](#).