

# Security Advisory

CVE-2023-21417 - 21.11.2023 (v1.0)



## Affected products, solutions, and services

- AXIS OS 8.50 – AXIS OS 11.6

## Summary

Sandro Poppi, member of the [AXIS OS Bug Bounty Program](#), has found that the VAPIX API `manageoverlayimage.cgi` was vulnerable to path traversal attacks that allows for file/folder 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 [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 11.7.57
- LTS 2022 10.12.208
- LTS 2020 9.80.49

The release notes will state the following:

*Addressed CVE-2023-21417. 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](#).