# Security Advisory

CVE-2023-21416 - 21.11.2023 (v1.0)

## Affected products, solutions, and services

- AXIS OS 10.7 – AXIS OS 11.6

## Summary

Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API *dynamicoverlay.cgi* was vulnerable to a Denial-of-Service attack allowing for an attacker to block access to the overlay configuration page in the web interface of the Axis device. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account however the impact is equal. 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 10.12.213

The release notes will state the following:
*Addressed CVE-2023-21416. 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.



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