

# Security Advisory



CVE-2023-5677 - 05.02.2024 (v1.0)

## Affected products, solutions, and services

- Axis devices running 5.50 - 5.51

## Summary

Brandon Rothel from [QED Secure Solutions](#) has found that the VAPIX API `tcptest.cgi` did not have a sufficient input validation allowing for a possible remote code execution. The impact of exploiting this vulnerability is lower with operator-privileges compared to administrator-privileges service accounts. For security reasons, Axis will not provide more detailed information about this 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 [6.3 \(Medium\)](#) 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 the following products:

- AXIS M3024-L 5.51.7.7
- AXIS M3025-VE 5.51.7.7
- AXIS M7014 5.51.7.7
- AXIS M7016 5.51.7.7
- AXIS P1214(-E) 5.51.7.7
- AXIS P7214 5.51.7.7
- AXIS P7216 5.51.7.7
- AXIS Q7401 5.51.7.7
- AXIS Q7404 5.51.7.7
- AXIS Q7414 5.51.7.7
- AXIS Q7424-R Mk II 5.51.3.9

Affected products with expired software support will not receive a patch.

The release notes will state the following:

*Addressed CVE-2023-5677. 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](#).