Security Advisory

CVE-2023-5677 - 14.05.2025 (v1.1)

Affected products, solutions, and services

- Axis devices running 5.50 - 5.51
- AXIS OS 6.50.0 - 6.50.5.20

Summary

Brandon Rothel from QED Secure Solutions and Sam Hanson of Dragos have 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.

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 6.3 (Medium) severity by using the CVSSv3.1 scoring system. CWE-78: Improper Neutralization of Special Elements used in an OS Command 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 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
- (Former LTS) 6.50.5.21 for products that are still under AXIS OS software support.

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. 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.

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