Security Advisory

CVE-2025-30023 - 11.07.2025 (v1.0)

Affected products, solutions, and services

- AXIS Camera Station Pro (<6.9)
- AXIS Camera Station (<5.58)
- AXIS Device Manager (<5.32)

Summary

Noam Moshe of Claroty Team82, has found that the communication protocol used between client and server had a flaw that could lead to an authenticated user performing a remote code execution attack.

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 9.0 (Critical) severity by using the CVSSv3.1 scoring system. CWE-502: Deserialization of Untrusted Data 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 this flaw with the following versions:

- AXIS Camera Station Pro 6.9
- AXIS Camera Station 5.58
- AXIS Device Manager 5.32

The release notes will state the following:
Addressed CVE-2025-30023. For more information, please visit the Axis vulnerability management portal.

It is recommended to update AXIS Camera Station Pro, AXIS Camera Station 5 or AXIS Device Manager. The latest versions of respective software can be found here, here or 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