Security Advisory

CVE-2024-7696 - 09.01.2025 (v1.0)

Affected products, solutions, and services

- AXIS Camera Station Pro (< 6.5)

Summary

Seth Fogie, member of AXIS Camera Station Pro Bug Bounty Program, has found that it is possible for an authenticated malicious client to tamper with audit log creation in AXIS Camera Station, or perform a Denial-of-Service attack on the AXIS Camera Station server using maliciously crafted audit log entries. For security reasons, Axis will not provide more detailed information about the 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. CWE-117: Improper Output Neutralization for Logs 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 patched version for affected AXIS OS versions on the following tracks:

- AXIS Camera Station 6.5

The release notes will state the following:
Addressed CVE-2024-7696. For more information, please visit the Axis vulnerability management portal.

It is recommended to update AXIS Camera Station Pro. The latest versions of respective 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