Security Advisory

CVE-2026-63287 – 2026-11-10 (v1.0)

Affected products, solutions, and services

- AXIS Camera Station Pro (< 6.18)
- AXIS Camera Station (< 5.59)

Summary

Maciej 'mace' Nowak, member of AXIS Camera Station Pro Bug Bounty Program, has found that it is possible for an authenticated non-admin user to modify certain data objects without having the appropriate permissions, which could be used to tamper with audit log creation in AXIS Camera Station.

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 6.5 (Medium) severity by using the CVSSv3.1 scoring system. CWE-117: Improper Output Neutralization for Logs and CWE-863: Incorrect Authorization 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 version:

- AXIS Camera Station Pro 6.18
- AXIS Camera Station 5.59

The release notes will state the following:
Addressed CVE-2026-63287. For more information, please visit the Axis vulnerability management portal.

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