Security Advisory

CVE-2024-6476 - 26.11.2024 (v1.0)

Affected products, solutions, and services

- AXIS Camera Station Pro (<6.4)
- AXIS Camera Station (<5.57.33556)

Summary

Gee-netics, member of the AXIS Camera Station Pro Bug Bounty Program has found that it is possible for a non-admin user to gain system privileges by redirecting a file deletion upon service restart. 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 Medium (4.2) severity by using the CVSSv3.1 scoring system. Learn more about the Common Vulnerability Scoring System here.

Solution & Mitigation

Axis has released the following patched versions:

- AXIS Camera Station Pro 6.4
- AXIS Camera Station 5.57.33556

The release notes will state the following:
Addressed CVE-2024-6476. 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 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