Affected products, solutions, and services

- AXIS Camera Station Pro (<6.8)

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 remove system files causing a boot loop by redirecting a file deletion when recording video.

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 5.9 (Medium) severity by using the CVSSv3.1 scoring system. CWE-732: Incorrect Permission Assignment for Critical Resource 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 the following patched version:

- AXIS Camera Station Pro 6.8

The release notes will state the following:
Addressed CVE-2025-0926. For more information, please visit the Axis vulnerability management portal

It is recommended to update AXIS Camera Station Pro. The latest versions can be found here. For further assistance and questions, please contact Axis Technical Support.