Security Advisory

CVE-2025-1056 - 25.04.2025 (v1.0)

Affected products, solutions, and services

- AXIS Camera Station Pro (<6.8)

Summary

Gee-netics, a member of the AXIS Camera Station Pro Bug Bounty Program has identified an issue with a specific file that the server is using. A non-admin user can modify this file to either create files or change the content of files in an admin-protected location.

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 Medium (6,1) severity by using the CVSSv3.1 scoring system. CWE-73: External Control of File Name or Path 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-2025-1056. 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.

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