Security Advisory

CVE-2025-9055 - 11.11.2025 (v1.0)

Affected products, solutions, and services

- AXIS OS 12.0.0 – AXIS OS 12.7.30

Summary

Malacupa, a member of the AXIS OS Bug Bounty Program, discovered a flaw in the *VAPIX Edge storage API* that allowed a privilege escalation, enabling a VAPIX administrator-privileged user to gain Linux Root privileges. This flaw can only be exploited after authenticating with an administrator-privileged service account.

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 6.4 (Medium) severity by using the CVSSv3.1 scoring system. CWE-250: Execution with Unnecessary Privileges 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 versions:

- Active Track 12.7.31

The release notes will state the following:
Addressed CVE-2025-9055. For more information, please visit the Axis vulnerability management portal.

Axis devices not included in these tracks and still under support will receive a patch according to their planned maintenance and release schedule.

It is recommended to update the Axis device software. The latest Axis device 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