Security Advisory

CVE-2026-8158 – 2026-08-11 (v1.0)

Affected products, solutions, and services

- Signed Video Framework: version 2.3.4 and earlier
- Signed media verifier: version 1.0.1 and earlier
- Axis File Player: version 3.1.8.0 and earlier

Summary

Anandppatil4383, a member of the AXIS OS Bug Bounty Program, has found a buffer overflow issue in the Signed Video Framework which could lead the application using this framework crash. The issue exclusively affects the tools used for the validation of signed content. The AXIS OS device's signed video functionality remains unaffected.

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 5.3 (Medium) severity by using the CVSSv3.1 scoring system. CWE-122: Heap-based Buffer Overflow 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 issue with the following versions:

- Signed-Video-Framework: version 2.3.5
- Signed media verifier: version 1.0.2
- Axis File Player: version 3.1.9.0

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