Security Advisory

CVE-2023-5800 - 05.02.2024 (v1.0)

Affected products, solutions, and services

- AXIS OS 6.50 – AXIS OS 11.7

Summary

Vintage, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API *create_overlay.cgi* did not have a sufficient input validation allowing for a possible remote code execution. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. To Axis' knowledge, there are no known exploits of the vulnerability at this time. 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 5.4 (Medium) severity by using the CVSSv3.1 scoring system. Learn more about the Common Vulnerability Scoring System here.

Solution & Mitigation

Axis has released a patch for affected AXIS OS versions on the following tracks:

- Active Track 11.8.61
- LTS 2022 10.12.220
- LTS 2020 9.80.55
- (Former LTS) 8.40.40 for products that are still under AXIS OS software support.
- (Former LTS) 6.50.5.16 for products that are still under AXIS OS software support.

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

The release notes will state the following:
Addressed CVE-2023-5800. For more information, please visit the Axis vulnerability management portal.

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.