

Security Advisory

CVE-2024-8160 - 26.11.2024 (v1.0)



Affected products, solutions, and services

- AXIS OS 10.9 - 12.0

Summary

Erik de Jong, member of the [AXIS OS Bug Bounty Program](#), has found that the VAPIX API `ftptest.cgi` did not have a sufficient input validation allowing for a possible command injection leading to being able to transfer files from/to the Axis device. This flaw can only be exploited after authenticating with an administrator-privileged service account.

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 [3.8 \(Low\)](#) 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 12.1.21
- LTS 2024 11.11.116
- LTS 2022 10.12.257

The release notes will state the following:

Addressed CVE-2024-8160. 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](#).