# Security Advisory

CVE-2025-10714 - 11.11.2025 (v1.0)

## Affected products, solutions, and services

- AXIS Optimizer 5.5.18.0 and lower

## Summary

Jonathan Eddy from Ark Data Centers, has discovered that the AXIS Optimizer was vulnerable to an unquoted search path vulnerability, which could potentially lead to privilege escalation within Microsoft Windows operating system. This vulnerability can only be exploited if the attacker has access to the local Windows machine and sufficient access rights (administrator) to write data into the installation path of AXIS Optimizer.

To Axis' knowledge, we are 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 8.4 (High) severity by using the CVSSv3.1 scoring system. CWE-428: Unquoted Search Path or Element have 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:

- AXIS Optimizer 5.6.0.0 or higher

The release notes will state the following:
*Addressed CVE-2025-10714. For more information, please visit the Axis vulnerability management portal.*

It is recommended to update AXIS Optimizer. The latest 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