Security Advisory

CVE-2023-21413 - 16.10.2023 (v1.0)

Affected products, solutions, and services

- AXIS OS 10.5 – 11.5

Summary

GoSecure on behalf of Genetec Inc. has found a flaw in AXIS OS 10.5 – 11.5 during penetration testing that allowed for a remote code execution during the installation of ACAP applications on the Axis device. ACAP applications can be installed with administrator-privileged accounts only. The application handling service in AXIS OS was vulnerable to command injection allowing an attacker to run arbitrary code. 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 9.1 (Critical) severity by using the CVSSv3.1 scoring system. Learn more about the Common Vulnerability Scoring System here.

Solution & Mitigation

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

- Active Track 11.6.94
- LTS 2022 10.12.199

The release notes will state the following:
Corrected CVE-2023-21413. 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.

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