Security Advisory

CVE-2023-21405 - 25.07.2023 (v1.0)

Affected devices, solutions, and services

• AXIS A1001	1.65.4 or earlier
• AXIS A1210 (-B)	11.0 - 11.6.16.0
• AXIS A1601	1.84.4 or earlier 10.12.171.0 or earlier 11.0 - 11.6.16.0
• AXIS A1610 (-B)	10.12.171.0 or earlier 11.0 - 11.6.16.0
• AXIS A8207	AXIS OS 10.12.178 or earlier AXIS OS 11.0 - 11.5.53
• AXIS A8207 MKII	AXIS OS 10.12.178 or earlier AXIS OS 11.0 - 11.5.53

Summary

Knud from Fraktal.fi has found a flaw in some Axis Network Door Controllers and Axis Network Intercoms when communicating over OSDP, highlighting that the OSDP message parser crashes the *pacsiod* process, causing a temporary unavailability of the door-controlling functionalities meaning that doors cannot be opened or closed. No sensitive or customer data can be extracted as the Axis device is not further compromised.

The vulnerability has been assigned a 6.5 (Medium) 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 devices that increases the robustness of the OSDP message parser and patches the highlighted flaw. For the AXIS A1601 it is recommended to update to the latest 10.12 VAPIX track or the 11.6 ACS Secure Entry track. The former 1.84 track is not supported and will not be patched.

The release notes will state the following:
Corrected CVE-2023-21405. 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