# Security Advisory

CVE-2023-21406 - 25.07.2023 (v1.0)

## Affected devices, solutions, and services

| | |
|---|---|
| AXIS A1001 | 1.65.4 or earlier |

## Summary

Ariel Harush and Roy Hodir from OTORIO have found a flaw in the AXIS A1001 when communicating over OSDP. A heap-based buffer overflow was found in the *pacsiod* process which is handling the OSDP communication allowing to write outside of the allocated buffer. By appending invalid data to an OSDP message it was possible to write data beyond the heap allocated buffer. The data written outside the buffer could be used to execute arbitrary code.

The vulnerability has been assigned a 7.1 (High) 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 robustness of the OSDP message parser and patches the highlighted flaw.

The release notes will state the following:
*Corrected CVE-2023-21406. 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.