Security Advisory

CVE-2026-63288 – 2026-11-10 (v1.0)

Affected products, solutions, and services

- AXIS A1210 - Secure Entry ≥ 11.7.12.2
- AXIS A1601 - Secure Entry ≥ 11.1.10.1
- AXIS A1610 - Secure Entry ≥ 11.4.32.2
- AXIS A1710 - Secure Entry ≥ 12.0.101.4
- AXIS A1810 - Secure Entry ≥ 12.0.101.4

Summary

Alardiians, a member of the AXIS OS Bug Bounty Program, has discovered an issue where a WebSocket request sent to a specific API endpoint allows unauthorized access to a separate API endpoint. This bypasses the intended authentication layer.

To Axis' knowledge, no known exploits exist publicly as of today and Axis is 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 8.3 (High) severity by using the CVSSv3.1 scoring system. CWE-306: Missing Authentication for Critical Function has 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:

- Secure Entry 12.11.106.1

The release notes will state the following:
Addressed CVE-2026-63288. 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