

Security Advisory

CVE-2025-13064 - 10.02.2026 (v1.0)



Affected products, solutions, and services

- AXIS Camera Station Pro (<6.14)

Summary

Seth Fogie, member of the AXIS Camera Station Pro Bug Bounty Program, has discovered that a server-side injection is possible for a malicious admin to manipulate the application to include a malicious script which is executed by the server. This attack is only possible if the admin uses a client that have been tampered with.

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 [4.5 \(Medium\)](#) severity by using the CVSSv3.1 scoring system. [CWE-248: Uncaught Exception](#) 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 the following patched versions:

- AXIS Camera Station Pro 6.14

The release notes will state the following:

Addressed CVE-2025-13064. For more information, please visit the [Axis vulnerability management portal](#).

It is recommended to update AXIS Camera Station Pro. The latest version can be found [here](#). For further assistance and questions, please contact [Axis Technical Support](#).