

Security Advisory

CVE-2026-63286 – 2026-10-28 (v1.0)



Affected products, solutions, and services

- AXIS Camera Station Pro (<6.20)
- AXIS Camera Station 5

Summary

Maciej 'mace' Nowak, a member of the AXIS Camera Station Pro Bug Bounty Program, reported that database backups are vulnerable to offline attacks.

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 CVSSv3.1 base score of [7.1 \(High\)](#). The underlying weakness has been mapped to [CWE-326: Inadequate Encryption Strength](#). 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 version:

- AXIS Camera Station Pro 6.20

Backups created using a version prior to the patched version are still vulnerable.

AXIS Camera Station Pro automatically creates one more such backup for recovery purpose when the update is applied. Delete all these backups and change the credentials stored in AXIS Camera Station Pro.

See the [AXIS Camera Station Pro - System hardening guide](#) and [AXIS Camera Station 5 - System hardening guide](#) for guidance on protecting backup storage.

The release notes will state the following:

Addressed CVE-2026-63286. 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](#).