Security Advisory

CVE-2023-21404 - 08.05.2023 (v1.0)

Affected products, solutions, and services

- AXIS OS 11.0.X - 11.3.x

Summary

Alexander Pick, member of the AXIS OS Bug Bounty Program, has found a flaw that does not follow Axis secure development best practices. A static RSA key was used to encrypt Axis-specific source code in legacy LUA-components. The encryption was applied to avoid non sensitive Axis-specific code from being easily human readable. The encryption using a static RSA key is not necessary since it is neither protecting sensitive data, nor can it be used to compromise Axis devices or customer data.

The vulnerability has been assigned a 4.1 (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 of AXIS OS (version 11.4.52) that removes the LUA-component. No patch will be made available for the long-term support (LTS) tracks as the LUA-components cannot be removed due to backwards compatibility reasons. Since the static RSA key is not protecting sensitive data, a non-patched AXIS OS version does not imply any practical risk.

The release notes will state the following:
Corrected CVE-2023-21404. For more information, please visit the Axis vulnerability management portal.

The latest AXIS OS can be found here. For further assistance and questions, please contact AXIS Technical Support.