Security Advisory

June 2018

ACV-128401

Source:

- VDOO Vulnerability disclosure
- CVE-2018-10658
- CVE-2018-10659
- CVE-2018-10660
- CVE-2018-10661
- CVE-2018-10662
- CVE-2018-10663
- CVE-2018-10664

Overview

By combining a number of discovered vulnerabilities an adversary may be able to compromise affected Axis products. Axis classifies these vulnerabilities as critical and recommends customers to upgrade affected Axis models to the latest firmware.

Risk assessment

A potential adversary needs network access to the device in order to exploit the vulnerabilities. An adversary does not require credentials to successfully compromise the device. The risk depends on how exposed the device is. Internet-facing device (e.g. exposed via router port-forward) are at high risk. Products deployed on a protected local network are at lower risk.

Risk mitigation

- It is strongly recommended to upgrade affected models to the latest firmware.
- It is not recommended to expose devices directly to the Internet (port-forwarding). Axis provides AXIS Companion, a free Windows/Android/iOS client that provides secure remote video access.
- Optionally apply IP filtering (which uses IP tables internally) in the devices to whitelist authorized clients. This mitigates risk for newly discovered vulnerabilities as well as the risk for compromised passwords.

Affected Models and patched firmware

Full list of affected models and patched firmware is available at https://www.axis.com/files/sales/ACV-128401_Affected_Product_List.pdf

To cost efficiently deploy the upgraded firmware, Axis recommends using the tool Axis Device Manager which will also continuously monitor and notify of available firmware.

Axis Communications AB, Emdalavägen 14, SE-223 69 Lund, Sweden
Tel: +46 46 272 18 00, Fax: +46 46 13 61 30, www.axis.com
Vat.No. SE 556253-614301