Security Announcement

April 13,2018

ACV-128401

External researchers have discovered a number of vulnerabilities in Axis products. An adversary with network access to an affected Axis product can, by combining these vulnerabilities, compromise the product. There are no indications that the exploit is known to anyone except the researchers and Axis.

As of April 13th 2018, Axis has begun publishing patched firmware for affected models. Axis strongly recommends end users to update firmware for affected Axis products in a controlled manner. To cost efficiently deploy the upgraded firmware, Axis recommends using the tool Axis Device Manager, which will continuously monitor and notify of available firmware.

The researchers intend to publish a report on June 18th, 2018 and Axis will publish a Security Advisory the same day. Affected models will have a patched firmware available well before this date.

At this point in time, Axis will not disclose any details about the vulnerabilities. This is solely to give our customers sufficient time to patch products and to reduce the risk of vulnerability exploit.

Products deployed with reduced network exposure such as placed behind a firewall, placed on an isolated network (VLAN or similar) or configured with an IP filter, as recommended in Axis Hardening Guide are at lower risk.

The patched firmware release notes have a reference to ACV-128401

List of affected models and patched firmware version