# Security Advisory

January 2019

# ACV- 147453 (AXIS A1001 Network Door Controller)

**Source:**

Critical flaw discovered by Axis Communications

**Overview**

An adversary that has network access to unpatched AXIS A1001 Network Door Controller devices using AXIS Entry Manager may be able to exploit a critical vulnerability. This exploit can be achieved without the need for authentication. Axis strongly recommends to patch AXIS A1001 devices with the latest available firmware.

**Risk assessment**

A potential adversary needs network access to the device in order to exploit the vulnerability, but does not require credentials to successfully compromise the device. The risk depends on how exposed the device is. Internet-facing devices (e.g. exposed via router port-forwarding) are at a high risk. Devices deployed on a protected local network are at lower risk. A skilled and motivated adversary may be able to attain remote code execution.

Details of the vulnerability are not known outside of Axis, and there are no public exploits (e.g. scripts or binaries) that target this flaw specifically.

**Risk mitigation**

- Customers are advised to upgrade AXIS A1001 devices to the latest firmware.
- It is not recommended to expose devices directly to the Internet (port-forwarding).
- Optionally apply IP filtering (which uses IP tables internally) in the devices to whitelist authorized clients.

**Affected Axis products and firmware**

AXIS A1001 using AXIS Entry Manager with firmware up to and including 1.65.1.1.

No other Axis device/model is affected.

**Patched Firmware**

Version 1.65.2 (or later) corrects the flaw. Firmware can be downloaded at https://www.axis.com/support/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