Security Advisory

July 2020

ACV-2020-100004

Affected Axis products

- AXIS S3008, running firmware 10.0.0 or earlier
- AXIS W800, running firmware 9.75.1 or earlier

Overview

During internal software security audits, Axis has discovered a flaw in the protection against device tampering (commonly known as Secure Boot) in AXIS S3008 and AXIS W800. This provides an opportunity for a sophisticated attack to bypass this protection.

Further information about secure boot in AXIS products can be read in our white paper on www.axis.com.

Risk assessment

A potential adversary needs either full administrative privileges or physical access to the device in order to exploit the flaw and requires high technical skills and motivation.

Action Plan

Axis has released unscheduled patches (firmware 10.0.3 for AXIS S3008 and firmware 9.75.1.1 for AXIS W800). It is recommended to update the affected products with the patched firmware, published at https://www.axis.com/support/firmware.

Note that a patched product will no longer support downgrade to previous firmware versions. For further assistance, please contact AXIS Technical Support https://www.axis.com/support.

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