Security Advisory

January 2022

CVE-2021-31988

Affected Axis products & solutions

CVE-2021-31988

- Axis devices with AXIS OS 5.51 or later

Overview

An external research team has found a flaw in the SMTP test functionality of the built-in event system in Axis devices. The vulnerability was discovered by Andrea Palanca from Nozomi Networks Inc.

CVE-2021-31988

The "subject" parameter of the HTTP request to the endpoint "/axis-cgi/smtptest.cgi", which is sent from the browser when the "Test" button of the "New recipient" tab is clicked to verify the network configuration of a newly-inserted recipient, resulted improperly validated by the server- side code, such that it was possible to add the Carriage Return and Line Feed (CRLF) control characters and include arbitrary SMTP headers in the generated test email.

Risk assessment

A potential adversary needs to have network access and administrator level access to the Axis device to exploit the vulnerability or needs to deceive a victim with administrator level access into visiting a specifically crafted webpage while logged in. He/she also requires some level of technical skills and motivation.

Action Plan

Axis will release patches on the following AXIS OS tracks:

- Active track 10.7
- 2016 LTS track 6.50.5.5
- 2018 LTS track 8.40.4.3
- 2020 LTS track 9.80.3.5
- 5.51.7.5

The release notes will state the following:

Corrected CVE-2021-31988. For more information, please visit the Axis product security portal.

Axis devices not included in these tracks and still under support will receive a patch according to their planned maintenance & release schedule. It is recommended to update; the latest AXIS OS version can be found here. For further assistance, please contact AXIS Technical 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