CVE-2021-31986

Affected Axis products & solutions

CVE-2021-31986

- Axis devices with AXIS OS 6.40 or later

Overview

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

CVE-2021-31986

A heap-based buffer overflow vulnerability was found in the read callback function (the function set via the libcurl "CURLOPT_READFUNCTION" option) of the "libhttp_smtp_notify.so" library. Notably, the read callback function failed to verify (as required in the official libcurl documentation) that no more than "size" multiplied with "items" number of bytes are copied in the libcurl destination buffer.

Additionally, among the copied bytes, the read callback function copied into the libcurl destination buffer the "to", "from", "subject" and "body" HTTP parameters of the 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. These parameters are externally controllable and were insufficiently validated by the server-side code prior to reaching the read callback function.

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 AXIS OS LTS & Active tracks:

- AXIS OS Active track 10.7
- AXIS OS 2016 LTS track 6.50.5.5
- AXIS OS 2018 LTS track 8.40.4.3
- AXIS OS 2020 LTS track 9.80.3.5

The release notes will state the following:

Corrected CVE-2021-31986. 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.