Security Advisory

October 2021

CVE-2021-31987

Affected Axis products & solutions

CVE-2021-31987

- Axis devices with AXIS OS 5.51 or later

Overview

An external research team has found a flaw in the test functions of the TCP-,HTTP- and SMTP-recipient handling of the built-in event system in Axis devices. The vulnerability was discovered by Andrea Palanca from Nozomi Networks Inc.

CVE-2021-31987

The test functionalities of HTTP, email, and TCP recipients have blocklist-based security checks to impede interactions with localhost-exposed network services which were possible to be circumvented with known bypasses. Furthermore, the test functionality of HTTP recipients did not prevent the user to define URLs with other schemes (e.g., "file://"). Finally, the test functionality of HTTPS recipients used the same checks designed for HTTP recipients only, which, as a consequence, were completely ineffective for HTTPS URLs.

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 10.8
- 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-2021-31987. 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, Gränden 1, 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