Security Advisory

Cross-Site Request Forgery (CSRF)

CSRF Overview: https://en.wikipedia.org/wiki/Cross-site_request_forgery
VAPIX overview: http://www.axis.com/se/sv/support/developer-support/vapix

During the time a user configures the Axis device using a web browser (Internet Explorer, EDGE, Chrome, Firefox, etc.) an attacker may be able to lure the user into accessing a malicious web site (prepped with crafted JavaScript) or trick them into clicking on a disguised link in a phishing email or an IM (Instant Message). If this occurs while the user has an authenticated session to the device (in another browser window or tab), the attack will ride on the already authenticated web browser session to send, for example, a VAPIX request with the same credential level as the logged in user. If the user is logged in as administrator the attacking code will have the ability to execute any VAPIX admin-related function, such as adding a new user. The malicious code/link must be crafted for a specific IP address/URL in order for such an attack to be successful.

The AXIS VAPIX HTTP API is integrated into a broad range of video applications/systems and it is not possible to add CSRF prevention mechanisms (typically found in other web server applications) without breaking VAPIX API compatibility.

Axis' recommendations for risk mitigation:

1. Access the device through an application such as a VMS. It is not possible to exploit the CSRF vulnerability when the device is accessed through an application. Axis provides a video client called AXIS Companion, free of charge.

2. The vulnerability can only be exploited when the user accesses the devices using a web browser. Axis does not recommend using a web browser as the primary video client, but if using a web browser, follow these guidelines:
    - Do not to visit untrusted websites or open emails from untrusted senders (this is of course a general cyber protection recommendation).
    - Use a different browser, which is not the system default, to configure the Axis device, since CSRF attacks cannot be exploited between different browsers.
    - Create a viewer account on the device and use this when viewing the video stream. The viewer account has minimal privileges which greatly reduces the impact of any CSRF exploit.
    - Close the browser after configuration in order to minimize the attack window.

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