Security Advisory

SECLISTS 170341 Multiple Vulnerabilities

Source: http://seclists.org/fulldisclosure/2017/Mar/41

Axis01: No cross-site request forgery protections

Axis cameras are vulnerable to CSRF-attacks. Please read the Security Advisory on CSRF.
https://www.axis.com/files/faq/Advisory_Cross-Site_Request_Forgery.pdf

Axis02: Bypass manual checks for XSS

This vulnerability is only applicable when using a browser, never with a video client or VMS. Submitted data (payload) to all input CGI's require authentication with appropriate privileges. The payload is not executed as shell commands without appropriate server side filtering. When data is requested back to browser it is always treated as string, never as script. Adding extensive server-side checks may restrict otherwise valid input such as Unicode characters from international languages.

Axis03: Web services run as root

As of firmware 5.70 (released March 2014) Axis replaced the webserver from Boa to Apache. Apache does not run as root.

Axis04: Script editor arbitrary write as root on successful CSRF attack

Exploiting the editcgi.cgi requires a successful CSRF attack (see Axis01 for mitigating CSRF).

Axis05: root setuid .CGI scripts and binaries present

As of firmware 5.70 (released March 2014) there are no setuid CGI's. All CGI's requiring root access run via a wrapper in Apache that prevents privilege escalation. In firmware prior to 5.70 an attacker will need viewer or operator credentials and identify a CGI with an exploitable vulnerability in order to use setuid to escalate privileges to root level.

Axis06: Inability to disable the http interface

When cameras are configured to only use HTTPS it is not possible to disable HTTP. In this case Axis recommends setting the HTTP port to a non-default private port number within the range 49152 - 65535 to reduce detection by port-scanning software.

Mitigation

- Use firmware 5.70 or later, preferably the latest applicable version
- Follow the Axis Hardening Guide
  https://www.axis.com/support/product-security
- Follow the CSRF Security Advisory
  https://www.axis.com/files/faq/Advisory_Cross-Site_Request_Forgery.pdf
- It is not recommended to expose the camera as a public accessible web server.