Vulnerability report

Lund, Sweden July 04, 2014

CVE-2014-0224, SSL/TLS MITM vulnerability

Description:

Extract from Open SSL Security Advisory

An attacker using a carefully crafted handshake can force the use of weak keying material in OpenSSL SSL/TLS clients and servers. This can be exploited by a Man-in-the-middle (MITM) attack where the attacker can decrypt and modify traffic from the attacked client and server.
The attack can only be performed between a vulnerable client *and* server. OpenSSL clients are vulnerable in all versions of OpenSSL. Servers are only known to be vulnerable in OpenSSL 1.0.1 and 1.0.2-beta1. Users of OpenSSL servers earlier than 1.0.1 are advised to upgrade as a precaution."

Affected products:

All cameras and encoders with firmware 4.xx to 5.5x.

Impact on systems and users:

The vulnerability cannot be exploited when the camera acts server and accessed over HTTPS (OpenSSL) - even if the client is using a vulnerable version of OpenSSL.

It may be possible to exploit the vulnerability when the camera acts as a client and uploads images or video via email or HTTPS - but only if the receiving server has not been patched to the latest OpenSSL.

Axis recommendations:

If the camera is configured to upload images/video over HTTPS or send email notifications, check if the receiving server has been patched with the latest OpenSSL version.

Axis plan:

Axis plan to include OpenSSL 0.9.8za in the 5.60 firmware release.

Related links:

http://www.openssl.org/news/secadv_20140605.txt
http://ccsinjection.lepidum.co.jp/

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