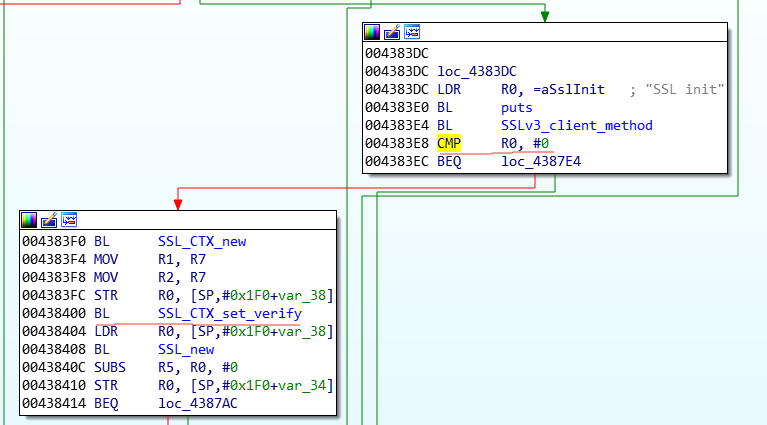
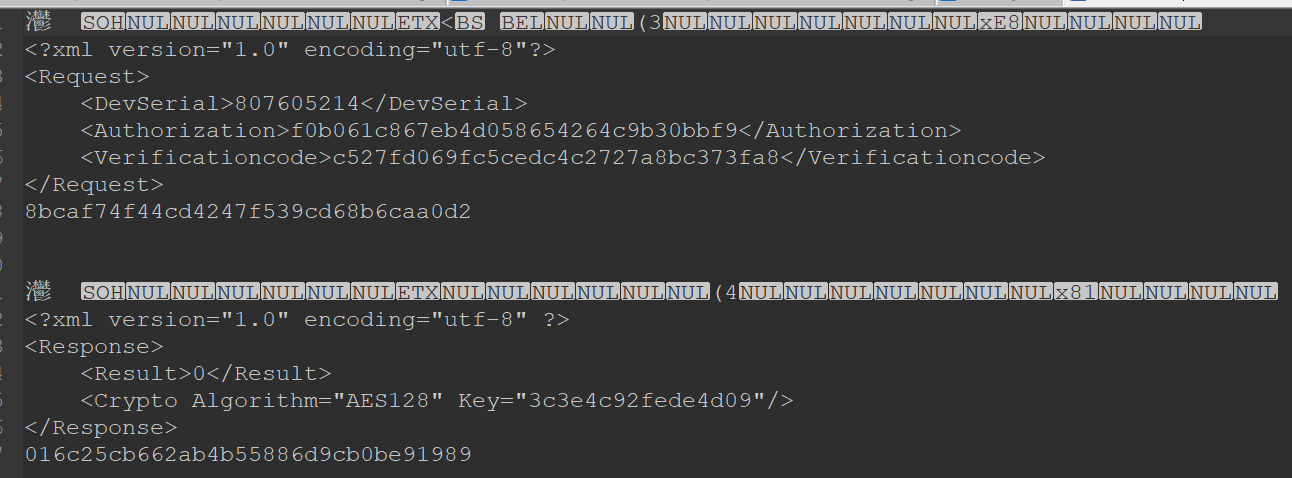
1. EZVIZ camera (CVE-2023-26850)

The application only calls SSL\_CTX\_set\_verify(SSL\_CTX \*ctx, int mode, SSL\_verify\_cb verify\_callback) to verify the server certificate. However, the application passes “SSL\_VERIFY\_NONE” to the mode flag which configure the application does not check the server certificate.



The following figure shows we can decrypt the traffic with Man-in-the-middle attack.



1. Hualai Xiaofang camera(CVE-2023-26849)

The application does not call any certificate verification APIs to verify the server certificate and make the application vulnerable to Man-in-the-middle attack.

The following figure shows we can decrypt the traffic with Man-in-the-middle attack.

