Account takeover with traffic monitoring exploitation in XM-JPR2-LX device

@ladinas, @chandlerchen

Affected versions:

Version $\leqslant$ V4.02.R12.A6420987.10002.147502.00000

Vulnerabilities Analysis:

0. Our target is the web app of the Xiongmai camera, which listen on the default 80 port.
1. With monitoring the whole traffic through wireshark, the login process of XM-JPR2-LX device is in plain text.
2. After authentication, SessionID is the only parameter to identify whether the user is legal or not.

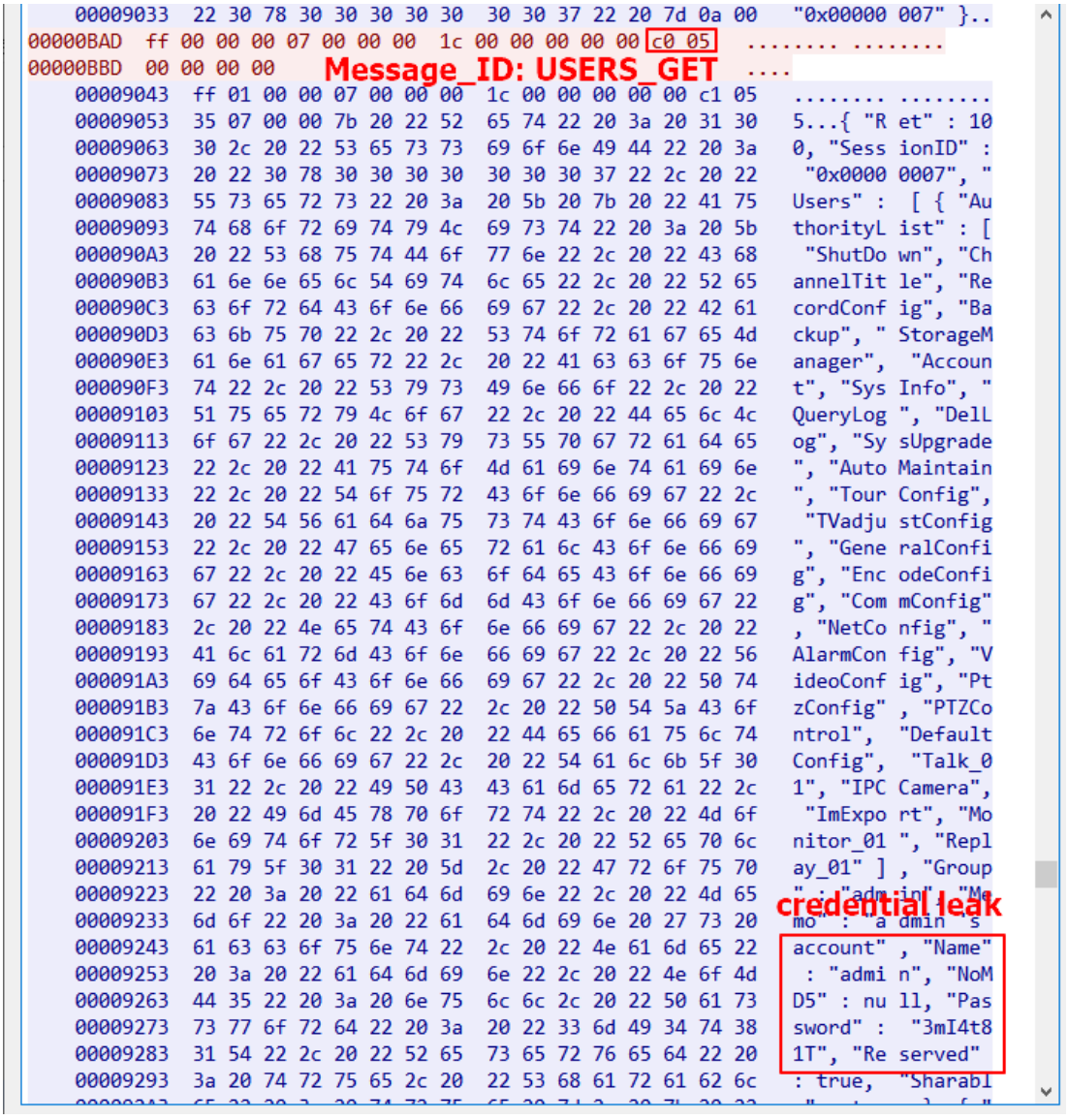
Steps to reproduce:

For exploitation, this vulnerability could be reproduced by the following steps:

1. Sniffing the target device’s traffic until getting the login data;

2. Developing a Python script to replay the login traffic;

3. After successful login, we can send arbitrary requests to obtain information or set configuration according to the specification (e.g., Sending a USERS_GET message to get all user credentials).



4.We open source our exploitation code as follows：

https://github.com/ChandlerChin/XiongmaiCamera/blob/main/XMJP_exp.py