



# Teledyne FLIR AX8 Backend subscriptions.php subscribe\_to\_alarm command injection

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2025-5695
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulDB
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-06-05 21:15:22 UTC
<b>Updated</b>	2026-04-29 01:00:01 UTC
<b>Description</b>	A vulnerability has been found in Teledyne FLIR AX8 up to 1.46.16. This impacts the function subscribe_to_spot/subscribe_

## Risk And Classification

**Primary CVSS:** v4.0 2 LOW from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-74 | CWE-77 | CWE-77 Command Injection | CWE-74 Injection

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	2	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	Secondary	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	4.7	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	5.8		AV:N/AC:L/Au:M/C:P/I:P/A:P
2.0	CNA	DECLARED	5.8		AV:N/AC:L/Au:M/C:P/I:P/A:P/E:POC/RL:OF/RC:C

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L

### CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Flir	Flir Ax8	-	All	All	All
Operating System	Flir	Flir Ax8 Firmware	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Teledyne FLIR	AX8	affected 1.46.0	Not specified
CNA	Teledyne FLIR	AX8	affected 1.46.1	Not specified
CNA	Teledyne FLIR	AX8	affected 1.46.2	Not specified
CNA	Teledyne FLIR	AX8	affected 1.46.3	Not specified
CNA	Teledyne FLIR	AX8	affected 1.46.4	Not specified
CNA	Teledyne FLIR	AX8	affected 1.46.5	Not specified
CNA	Teledyne FLIR	AX8	affected 1.46.6	Not specified
CNA	Teledyne FLIR	AX8	affected 1.46.7	Not specified
CNA	Teledyne FLIR	AX8	affected 1.46.8	Not specified
CNA	Teledyne FLIR	AX8	affected 1.46.9	Not specified
CNA	Teledyne FLIR	AX8	affected 1.46.10	Not specified
CNA	Teledyne FLIR	AX8	affected 1.46.11	Not specified
CNA	Teledyne FLIR	AX8	affected 1.46.12	Not specified
CNA	Teledyne FLIR	AX8	affected 1.46.13	Not specified
CNA	Teledyne FLIR	AX8	affected 1.46.14	Not specified
CNA	Teledyne FLIR	AX8	affected 1.46.15	Not specified

CNA	Teledyne FLIR	AX8	affected 1.46.16	Not specified
CNA	Teledyne FLIR	AX8	unaffected 1.49.16	Not specified

## References

Reference	Source	Link	Tags
vuldb.com	cna@vuldb.com	<a href="https://vuldb.com">vuldb.com</a>	Third Party Advis
vuldb.com	cna@vuldb.com	<a href="https://vuldb.com">vuldb.com</a>	Third Party Advis
vuldb.com	cna@vuldb.com	<a href="https://vuldb.com">vuldb.com</a>	Third Party Advis
github.com/YZS17/CVE/blob/main/Command%20injection%20vulnerability%20in%...	cna@vuldb.com	<a href="https://github.com">github.com</a>	Exploit
github.com/YZS17/CVE/blob/main/Command%20injection%20vulnerability%20in%...	cna@vuldb.com	<a href="https://github.com">github.com</a>	Exploit
vuldb.com	cna@vuldb.com	<a href="https://vuldb.com">vuldb.com</a>	Permissions Rec
flir.custhelp.com/app/account/fl_download_software	cna@vuldb.com	<a href="https://flir.custhelp.com">flir.custhelp.com</a>	Permissions Rec
vuldb.com	cna@vuldb.com	<a href="https://vuldb.com">vuldb.com</a>	Third Party Advis
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analy

## Vendor Comments And Credit

Discovery Credit  
**CNA: XU17 (VulDB User) (en)**

## Additional Advisory Data

Source	Time	Event
CNA	2025-06-04T00:00:00.000Z	Advisory disclosed
CNA	2025-06-04T02:00:00.000Z	VulDB entry created
CNA	2025-10-15T15:23:22.000Z	VulDB entry last update

There are currently no legacy QID mappings associated with this CVE.