



# Teledyne FLIR AX8 User Registration test\_login.php improper authorization

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

## Summary

<b>CVE</b>	CVE-2024-3013
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulDB
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-03-28 01:15:47 UTC
<b>Updated</b>	2026-04-29 01:00:01 UTC
<b>Description</b>	A flaw has been found in Teledyne FLIR AX8 up to 1.46.16. The impacted element is an unknown function of the file /tools/

## Risk And Classification

**Primary CVSS:** v4.0 2.1 LOW from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/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-266 | CWE-285 | CWE-285 Improper Authorization | CWE-266 Incorrect Privilege Assignment

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	2.1	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vuldb.com	Secondary	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	6.3	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	6.5		AV:N/AC:L/Au:S/C:P/I:P/A:P
2.0	CNA	DECLARED	6.5		AV:N/AC:L/Au:S/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

Low

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:L/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

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### CVSS v3.0 Breakdown

Attack Vector

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:L/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
ADP	Flir	Flir Ax8 Firmware	affected 1.46.0	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.1	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.10	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.11	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.12	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.13	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.14	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.15	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.16	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.2	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.3	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.4	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.5	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.6	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.7	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.8	Not specified
ADP	Flir	Flir Ax8 Firmware	affected 1.46.9	Not specified

## References

Reference	Source
vuldb.com	af854a3a-2127-422b-91ae-364da266110f
h0e4a0r1t.github.io/2024/vulns/FLIR-AX8%20Fixed%20Thermal%20Cameras%20Register%20...	af854a3a-2127-422b-91ae-364da266110f
vuldb.com	af854a3a-2127-422b-91ae-364da266110f
vuldb.com	af854a3a-2127-422b-91ae-364da266110f
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

## Vendor Comments And Credit

### Discovery Credit

**CNA:** H0e4a0r1t (VulDB User) (en)

## Additional Advisory Data

Source	Time	Event
CNA	2024-03-27T00:00:00.000Z	Advisory disclosed
CNA	2024-03-27T00:00:00.000Z	CVE reserved
CNA	2024-03-27T01:00:00.000Z	VulDB entry created
CNA	2025-10-15T15:23:29.000Z	VulDB entry last update

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)