



# Fuji Electric Tellus Exposed Dangerous Method or Function

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

## Summary

<b>CVE</b>	CVE-2026-8108
<b>State</b>	PUBLISHED
<b>Assigner</b>	icscert
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-12 23:16:19 UTC
<b>Updated</b>	2026-05-13 15:52:56 UTC
<b>Description</b>	The installation of Fuji Tellus adds a driver to the kernel which grants all users read and write permissions.

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from ics-cert@hq.dhs.gov

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

**EPSS:** 0.000050000 probability, percentile 0.002180000 (date 2026-05-17)

**Problem Types:** CWE-749 | CWE-749 CWE-749

Version	Source	Type	Score	Severity	Vector
3.1	ics-cert@hq.dhs.gov	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Fuji Electric	Tellus	affected 5.0.2	Not specified

### References

Reference	Source	Link	Tags
github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-13...	ics-cert@hq.dhs.gov	github.com	
www.cisa.gov/news-events/ics-advisories/icsa-26-132-01	ics-cert@hq.dhs.gov	www.cisa.gov	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Kim Myung-gyu of Trend Micro Zero Day Initiative reported this vulnerability to CISA.  
(en)

### Additional Advisory Data

#### Workarounds

**CNA:** Fuji Electric recommends that Tellus be installed only with administrator privileges.

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](#)