



Out-of-bounds Read Overflow in tildearrow/furnace

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

Summary

CVE	CVE-2026-4732
State	PUBLISHED
Assigner	GovTech CSG
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-24 04:17:25 UTC
Updated	2026-04-30 16:01:57 UTC
Description	Out-of-bounds Read vulnerability in tildearrow furnace (extern/libsndfile-modified/src modules). This vulnerability is associat

Risk And Classification

Primary CVSS: v4.0 8.4 HIGH from cve_disclosure@tech.gov.sg

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/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:N/AU:N/R:U/V:D/RE:L/U:Amber

EPSS: 0.000200000 probability, percentile 0.056860000 (date 2026-05-05)

Problem Types: CWE-125 | CWE-125 CWE-125 Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
4.0	cve_disclosure@tech.gov.sg	Secondary	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/S
4.0	CNA	CVSS	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/S

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/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:N/AU:N/R:U/V:D/RE:L/U:Amber

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Tildearrow	Furnace	affected 0.7 git	Not specified

References

Reference	Source	Link	Tags
github.com/tildearrow/furnace/pull/2812	cve_disclosure@tech.gov.sg	github.com	
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: TITAN Team (titancaproject@gmail.com) (en)

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