



# CVE-2017-17973

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

## Summary

<b>CVE</b>	CVE-2017-17973
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-12-29 21:29:00 UTC
<b>Updated</b>	2025-04-20 01:37:25 UTC
<b>Description</b>	In LibTIFF 4.0.8, there is a heap-based use-after-free in the t2p_writeproc function in tiff2pdf.c. NOTE: there is a third-party

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from ADP

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

**Problem Types:** CWE-416 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.0	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Libtiff</a>	<a href="#">Libtiff</a>	4.0.8	All	All	All

  

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	<a href="#">Na</a>	<a href="#">N/a</a>	affected n/a	Not specified		

  

References	
Reference	Source
Bug 2769 – There is a heap-use-after-free in t2p_writeproc function in tiff2pdf.c line 405 (CVE-2017-17973)	<a href="#">af854a3a-2127-422b-91ae-364</a>
Malformed Request	<a href="#">af854a3a-2127-422b-91ae-364</a>
Access Denied	<a href="#">af854a3a-2127-422b-91ae-364</a>
1530912 – (CVE-2017-17973) CVE-2017-17973 libtiff: heap-based use after free in tiff2pdf.c:t2p_writeproc	<a href="#">af854a3a-2127-422b-91ae-364</a>
CVE Program record	<a href="#">CVE.ORG</a>
NVD vulnerability detail	<a href="#">NVD</a>

  

No vendor comments have been submitted for this CVE.

  

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](#)