



# CVE-2018-17795

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

## Summary

<b>CVE</b>	CVE-2018-17795
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-09-30 20:29:00 UTC
<b>Updated</b>	2020-10-16 20:15:00 UTC
<b>Description</b>	The function t2p_write_pdf in tiff2pdf.c in LibTIFF 4.0.9 and earlier allows remote attackers to cause a denial of service (hea

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libtiff	Libtiff	4.0.9	All	All	All
Application	Libtiff	Libtiff	4.0.9	All	All	All

## References

Reference	Source
LibTIFF CVE-2018-17795 Heap Based Buffer Overflow Vulnerability	BID
Pocs_for_Multi_Versions/CVE-2018-17795 at main · Hack-Me/Pocs_for_Multi_Versions · GitHub	MISC
Bug 2816 – heap-buffer-overflow problem in function t2p_write_pdf() in tiff2pdf.c, a different bug than 2704(CVE-2018-17795)	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

296091 Oracle Solaris 11.4 Support Repository Update (SRU) 6.1.4 Missing (CPUJAN2019)

© [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](#).

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