



CVE-2018-5360

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

Summary

CVE	CVE-2018-5360
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-14 02:29:00 UTC
Updated	2019-04-22 16:25:00 UTC
Description	LibTIFF before 4.0.6 mishandles the reading of TIFF files, as demonstrated by a heap-based buffer over-read in the ReadT

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Graphicsmagick	Graphicsmagick	1.3.27	All	All	All
Application	Graphicsmagick	Graphicsmagick	1.3.27	All	All	All
Application	Libtiff	Libtiff	All	All	All	All
Application	Libtiff	Libtiff	All	All	All	All

References

Reference	Source	Link	T
Bug 2500 – CVE-2014-8127 libtiff: Out-of-bounds Read in the tiffset tool	MISC	bugzilla.maptools.org	E
* libtiff/tif_dir.c: discard values of SMinSampleValue and (739dcd28) · Commits · libtiff / libtiff · GitLab	CONFIRM	gitlab.com	P
GraphicsMagick / Bugs / #540 gm: heap-buffer-overflow in ReadTIFFImage (src/coders/tiff.c)	MISC	sourceforge.net	E
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

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](#)