



CVE-2017-9348

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2017-9348
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-02 05:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	In Wireshark 2.2.0 to 2.2.6, the DOF dissector could read past the end of a buffer. This was addressed in epan/dissectors/p

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	All	All	All	All

References

Reference	Source	Lin
Wireshark · wnpa-sec-2017-23 · DOF dissector read overflow	MISC	ww
Wireshark 'epan/dissectors/packet-dof.c' Heap Buffer Overflow Vulnerability	BID	ww
13608 – [oss-fuzz] ASAN: heap-buffer-overflow epan/dissectors/packet-dof.c:3899:32 in OALMarshal_UncompressValue	MISC	buq
1151 - wireshark: Heap-buffer-overflow in OALMarshal_UncompressValue - oss-fuzz - Monorail	MISC	buq
code.wireshark Code Review - wireshark.git/commit		coc
Wireshark Multiple Dissector Bugs Lets Remote Users Deny Service - SecurityTracker	SECTRACK	ww
code.wireshark Code Review - wireshark.git/commit	MISC	coc
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [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](#)