



CVE-2017-9354

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

Summary

CVE	CVE-2017-9354
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 and 2.0.0 to 2.0.12, the RGMP dissector could crash. This was addressed in epan/dissectors/pa

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
13646 – [oss-fuzz] UBSAN: null pointer passed as argument 1, which is declared to never be null in packet-rgmp.c:73:16	MISC	bu
1243 - wireshark: Crash in dissect_rgmp - oss-fuzz - Monorail	MISC	bu
code.wireshark Code Review - wireshark.git/commit		co
Wireshark · wnpa-sec-2017-32 · RGMP dissector crash	MISC	ww
Wireshark Multiple Dissector Bugs Lets Remote Users Deny Service - SecurityTracker	SECTRACK	ww
code.wireshark Code Review - wireshark.git/commit	MISC	co
Wireshark 'epan/dissectors/packet-rgmp.c' Denial of Service Vulnerability	BID	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

501301 Alpine Linux Security Update for wireshark

© [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](#)