



# CVE-2017-9345

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

## Summary

<b>CVE</b>	CVE-2017-9345
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-06-02 05:29:00 UTC
<b>Updated</b>	2023-11-07 02:50:00 UTC
<b>Description</b>	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the DNS dissector could go into an infinite loop. This was addressed in epar

## Risk And Classification

**Problem Types:** CWE-835

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source	Link	Tags
Wireshark 'epan/dissectors/packet-dns.c' Denial of Service Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Pa
13633 – [oss-fuzz] timeout: expand_dns_name epan/dissectors/packet-dns.c:1158:21	MISC	<a href="http://bugs.wireshark.org">bugs.wireshark.org</a>	Issue Tr
code.wireshark Code Review - wireshark.git/commit	MISC	<a href="http://code.wireshark.org">code.wireshark.org</a>	Issue Tr
Wireshark · wnpa-sec-2017-26 · DNS dissector infinite loop	MISC	<a href="http://www.wireshark.org">www.wireshark.org</a>	Vendor /
Wireshark Multiple Dissector Bugs Lets Remote Users Deny Service - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.securitytracker.com</a>	Third Pa
1206 - wireshark: Timeout in wireshark_fuzzshark_udp_port-bootp - oss-fuzz - Monorail	MISC	<a href="http://bugs.chromium.org">bugs.chromium.org</a>	Issue Tr
code.wireshark Code Review - wireshark.git/commit		<a href="http://code.wireshark.org">code.wireshark.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonica
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonica

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

501301 Alpine Linux Security Update for wireshark

671108 EulerOS Security Update for wireshark (EulerOS-SA-2019-2425)

© [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](#)