



# CVE-2017-7701

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

## Summary

<b>CVE</b>	CVE-2017-7701
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-04-12 23:59:00 UTC
<b>Updated</b>	2023-11-07 02:50:00 UTC
<b>Description</b>	In Wireshark 2.2.0 to 2.2.5 and 2.0.0 to 2.0.11, the BGP dissector could go into an infinite loop, triggered by packet injection

## Risk And Classification

**Problem Types:** CWE-835

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	2.0.0	All	All	All
Application	Wireshark	Wireshark	2.0.1	All	All	All
Application	Wireshark	Wireshark	2.0.10	All	All	All
Application	Wireshark	Wireshark	2.0.11	All	All	All
Application	Wireshark	Wireshark	2.0.2	All	All	All
Application	Wireshark	Wireshark	2.0.3	All	All	All
Application	Wireshark	Wireshark	2.0.4	All	All	All
Application	Wireshark	Wireshark	2.0.5	All	All	All
Application	Wireshark	Wireshark	2.0.6	All	All	All
Application	Wireshark	Wireshark	2.0.7	All	All	All
Application	Wireshark	Wireshark	2.0.8	All	All	All
Application	Wireshark	Wireshark	2.0.9	All	All	All
Application	Wireshark	Wireshark	2.2.0	All	All	All
Application	Wireshark	Wireshark	2.2.1	All	All	All
Application	Wireshark	Wireshark	2.2.2	All	All	All
Application	Wireshark	Wireshark	2.2.3	All	All	All
Application	Wireshark	Wireshark	2.2.4	All	All	All

Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.2.5	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.0.0	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.0.1	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.0.10	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.0.11	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.0.2	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.0.3	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.0.4	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.0.5	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.0.6	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.0.7	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.0.8	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.0.9	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.2.0	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.2.1	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.2.2	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.2.3	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.2.4	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.2.5	All	All	All

## References

Reference	Source	Link	Tags
code.wireshark Code Review - wireshark.git/commit	CONFIRM	<a href="https://code.wireshark.org">code.wireshark.org</a>	Issue Tracking, Patch
Wireshark Multiple Bugs Lets Remote Users Deny Service - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.securitytracker.com</a>	
Wireshark · wnpa-sec-2017-16 · BGP dissector infinite loop	CONFIRM	<a href="http://www.wireshark.org">www.wireshark.org</a>	Vendor Advisory
Wireshark: Multiple vulnerabilities (GLSA 201706-12) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	
code.wireshark Code Review - wireshark.git/commit		<a href="https://code.wireshark.org">code.wireshark.org</a>	
Wireshark BGP dissector Infinite Loop Denial of Service Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory
13557 – libfuzzer: BGP dissector loop	CONFIRM	<a href="https://bugs.wireshark.org">bugs.wireshark.org</a>	Issue Tracking, Patch
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

501300 Alpine Linux Security Update for wireshark

710400 Gentoo Linux Wireshark Multiple Vulnerabilities (GLSA 201706-12)

© [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](#)**