



# CVE-2018-14342

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-14342
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-07-19 02:29:00 UTC
<b>Updated</b>	2023-11-07 02:52:00 UTC
<b>Description</b>	In Wireshark 2.6.0 to 2.6.1, 2.4.0 to 2.4.7, and 2.2.0 to 2.2.15, the BGP protocol dissector could go into a large loop. This w

## Risk And Classification

**Problem Types:** CWE-834

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
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
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	All	All	All	All

## References

### Reference

[SECURITY] [DLA 1451-1] wireshark security update
code.wireshark Code Review - wireshark.git/commit
Wireshark Bugs in Multiple Dissectors Let Remote Users Cause the Application to Crash or Consume Excessive CPU Resources - SecurityTr
13741 – [oss-fuzz] Dissector bug, protocol BGP, in packet 1: More than 1000000 items in the tree -- possible infinite loop
code.wireshark Code Review - wireshark.git/commit
Wireshark Multiple Denial of Service Vulnerabilities
[security-announce] openSUSE-SU-2020:0362-1: moderate: Security update f
Wireshark · wnpa-sec-2018-34 · BGP dissector large loop
CVE Program record

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

296066 Oracle Solaris 11.4 Support Repository Update (SRU) 40.107.3 Missing (CPUOCT2021)

501310 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](#)