



# CVE-2017-6014

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

## Summary

<b>CVE</b>	CVE-2017-6014
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-02-17 07:59:00 UTC
<b>Updated</b>	2019-10-03 00:03:00 UTC
<b>Description</b>	In Wireshark 2.2.4 and earlier, a crafted or malformed STANAG 4607 capture file will cause an infinite loop and memory ex

## Risk And Classification

**Problem Types:** CWE-835

## 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

## References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-3811-1 wireshark	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Third Party Advis
Wireshark CVE-2017-6014 Denial of Service Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advis
Wireshark: Multiple vulnerabilities (GLSA 201706-12) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	Third Party Advis
13416 – memory exhaustion/infinite loop via malformed STANAG 4607 capture file	CONFIRM	<a href="http://bugs.wireshark.org">bugs.wireshark.org</a>	Issue Tracking, V
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, analys

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[501298](#) 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](#)