

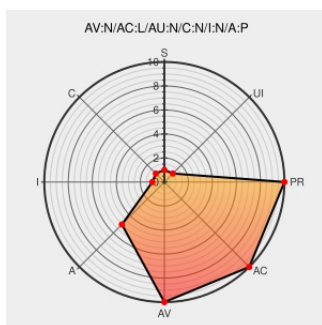


CVE-2014-5163

Published on: 08/01/2014 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:20:00 AM UTC

CVE-2014-5163

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Wireshark](#) from [Wireshark](#) contain the following vulnerability:

The APN decode functionality in (1) epan/dissectors/packet-gtp.c and (2) epan/dissectors/packet-gsm_a_gm.c in the GTP and GSM Management dissectors in Wireshark 1.10.x before 1.10.9 does not completely initialize a certain buffer, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.

CVE-2014-5163 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

code.wireshark Code Review -
wireshark.git/commit

[code.wireshark.org](#)
[text/xml](#)

CONFIRM [code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=dd7134d907350ccc574cdec596f4162860912bb9](#)

Debian -- Security Information -- DSA-
3002-1 wireshark

[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

DEBIAN DSA-3002

openSUSE-SU-2014:1038-1:
moderate: update for wireshark

[lists.opensuse.org](#)
[text/html](#)

SUSE openSUSE-SU-2014:1038

Security Advisory SA57593 - Debian
update for wireshark - Secunia

[web.archive.org](#)
[text/html](#)

SECUNIA 57593

Wireshark · wnpa-sec-2014-09 · GTP
and GSM Management dissector

[Vendor Advisory](#)
[www.wireshark.org](#)

CONFIRM [www.wireshark.org/security/wnpa-sec-2014-09.html](#)

crash	text/html	
code.wireshark Code Review - wireshark.git/commit	Patch code.wireshark.org text/xml	 CONFIRM code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=3fc441e7a5008640c68ec985e669d5092414a519
[security-announce] SUSE-SU-2014:1221-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2014:1221
10216 – Buildbot crash output: fuzz-2014-06-20-5084.pcap	Exploit bugs.wireshark.org text/html	 CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=10216
openSUSE-SU-2014:1249-1: moderate: wireshark: update to 1.10.10 security	lists.opensuse.org text/html	 SUSE openSUSE-SU-2014:1249

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	1.10.0	All	All	All
Application	Wireshark	Wireshark	1.10.1	All	All	All
Application	Wireshark	Wireshark	1.10.2	All	All	All
Application	Wireshark	Wireshark	1.10.3	All	All	All
Application	Wireshark	Wireshark	1.10.4	All	All	All
Application	Wireshark	Wireshark	1.10.5	All	All	All
Application	Wireshark	Wireshark	1.10.6	All	All	All
Application	Wireshark	Wireshark	1.10.7	All	All	All
Application	Wireshark	Wireshark	1.10.8	All	All	All
Application	Wireshark	Wireshark	1.10.0	All	All	All
Application	Wireshark	Wireshark	1.10.1	All	All	All
Application	Wireshark	Wireshark	1.10.2	All	All	All
Application	Wireshark	Wireshark	1.10.3	All	All	All
Application	Wireshark	Wireshark	1.10.4	All	All	All
Application	Wireshark	Wireshark	1.10.5	All	All	All
Application	Wireshark	Wireshark	1.10.6	All	All	All
Application	Wireshark	Wireshark	1.10.7	All	All	All
Application	Wireshark	Wireshark	1.10.8	All	All	All

cpe:2.3:a:wireshark:wireshark:1.10.0:*****:
cpe:2.3:a:wireshark:wireshark:1.10.1:*****:
cpe:2.3:a:wireshark:wireshark:1.10.2:*****:
cpe:2.3:a:wireshark:wireshark:1.10.3:*****:
cpe:2.3:a:wireshark:wireshark:1.10.4:*****:
cpe:2.3:a:wireshark:wireshark:1.10.5:*****:
cpe:2.3:a:wireshark:wireshark:1.10.6:*****:
cpe:2.3:a:wireshark:wireshark:1.10.7:*****:
cpe:2.3:a:wireshark:wireshark:1.10.8:*****:
cpe:2.3:a:wireshark:wireshark:1.10.0:*****:
cpe:2.3:a:wireshark:wireshark:1.10.1:*****:
cpe:2.3:a:wireshark:wireshark:1.10.2:*****:
cpe:2.3:a:wireshark:wireshark:1.10.3:*****:
cpe:2.3:a:wireshark:wireshark:1.10.4:*****:
cpe:2.3:a:wireshark:wireshark:1.10.5:*****:
cpe:2.3:a:wireshark:wireshark:1.10.6:*****:
cpe:2.3:a:wireshark:wireshark:1.10.7:*****:
cpe:2.3:a:wireshark:wireshark:1.10.8:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

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