

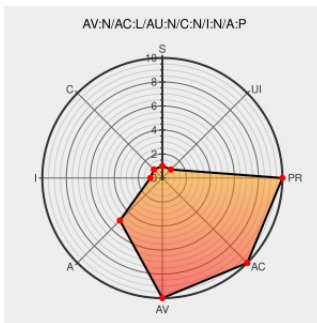


CVE-2012-6061

Published on: 12/05/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:22 PM UTC

CVE-2012-6061

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

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

The dissect_wtp_common function in epan/dissectors/packet-wtp.c in the WTP dissector in Wireshark 1.6.x before 1.6.12 and 1.8.x before 1.8.4 uses an incorrect data type for a certain length field, which allows remote attackers to cause a denial of service (integer overflow and infinite loop) via a crafted value in a packet.

CVE-2012-6061 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
openSUSE-SU-2013:0151-1: moderate: wireshark to 1.8.4	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0151
Wireshark · wnpa-sec-2012-37	Vendor Advisory www.wireshark.org text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2012-37.html
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:0341
7869 – Buildbot crash output: fuzz- 2012-10-16-24396.pcap	Exploit Vendor Advisory bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=7869

Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org/mitre.oval:def:15253
code.wireshark Code Review - wireshark.git/tree	Exploit Vendor Advisory anonsvn.wireshark.org text/xml	 CONFIRM anonsvn.wireshark.org/viewvc/trunk/epan/dissectors/packet-wtp.c?r1=45614&r2=45613&pathrev=45614
openSUSE-SU-2012:1633-1: moderate: wireshark to 1.8.4	lists.opensuse.org text/html	 SUSE openSUSE-SU-2012:1633
code.wireshark Code Review - wireshark.git/tree	anonsvn.wireshark.org text/xml	 CONFIRM anonsvn.wireshark.org/viewvc?view=revision&revision=45614
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	1.6.0	All	All	All
Application	Wireshark	Wireshark	1.6.1	All	All	All
Application	Wireshark	Wireshark	1.6.10	All	All	All
Application	Wireshark	Wireshark	1.6.11	All	All	All
Application	Wireshark	Wireshark	1.6.2	All	All	All
Application	Wireshark	Wireshark	1.6.3	All	All	All
Application	Wireshark	Wireshark	1.6.4	All	All	All
Application	Wireshark	Wireshark	1.6.5	All	All	All
Application	Wireshark	Wireshark	1.6.6	All	All	All
Application	Wireshark	Wireshark	1.6.7	All	All	All
Application	Wireshark	Wireshark	1.6.8	All	All	All
Application	Wireshark	Wireshark	1.6.9	All	All	All
Application	Wireshark	Wireshark	1.8.0	All	All	All
Application	Wireshark	Wireshark	1.8.1	All	All	All
Application	Wireshark	Wireshark	1.8.2	All	All	All
Application	Wireshark	Wireshark	1.8.3	All	All	All
Application	Wireshark	Wireshark	1.6.0	All	All	All
Application	Wireshark	Wireshark	1.6.1	All	All	All
Application	Wireshark	Wireshark	1.6.10	All	All	All
Application	Wireshark	Wireshark	1.6.11	All	All	All

Application	Wireshark	Wireshark	1.6.2	All	All	All
Application	Wireshark	Wireshark	1.6.3	All	All	All
Application	Wireshark	Wireshark	1.6.4	All	All	All
Application	Wireshark	Wireshark	1.6.5	All	All	All
Application	Wireshark	Wireshark	1.6.6	All	All	All
Application	Wireshark	Wireshark	1.6.7	All	All	All
Application	Wireshark	Wireshark	1.6.8	All	All	All
Application	Wireshark	Wireshark	1.6.9	All	All	All
Application	Wireshark	Wireshark	1.8.0	All	All	All
Application	Wireshark	Wireshark	1.8.1	All	All	All
Application	Wireshark	Wireshark	1.8.2	All	All	All
Application	Wireshark	Wireshark	1.8.3	All	All	All
cpe:2.3:a:wireshark:wireshark:1.6.0:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.6.1:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.6.10:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.6.11:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.6.2:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.6.3:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.6.4:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.6.5:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.6.6:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.6.7:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.6.8:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.6.9:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.0:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.1:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.2:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.3:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.6.0:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.6.1:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.6.10:*:*:*:*:*:						

cpe:2.3:a:wireshark:wireshark:1.6.11:*****:
cpe:2.3:a:wireshark:wireshark:1.6.2:*****:
cpe:2.3:a:wireshark:wireshark:1.6.3:*****:
cpe:2.3:a:wireshark:wireshark:1.6.4:*****:
cpe:2.3:a:wireshark:wireshark:1.6.5:*****:
cpe:2.3:a:wireshark:wireshark:1.6.6:*****:
cpe:2.3:a:wireshark:wireshark:1.6.7:*****:
cpe:2.3:a:wireshark:wireshark:1.6.8:*****:
cpe:2.3:a:wireshark:wireshark:1.6.9:*****:
cpe:2.3:a:wireshark:wireshark:1.8.0:*****:
cpe:2.3:a:wireshark:wireshark:1.8.1:*****:
cpe:2.3:a:wireshark:wireshark:1.8.2:*****:
cpe:2.3:a:wireshark:wireshark:1.8.3:*****:

No vendor comments have been submitted for this CVE

← Previous IDNext ID →