



CVE-2012-6056

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

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

CVE-2012-6056

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Integer overflow in the dissect_sack_chunk function in epan/dissectors/packet-sctp.c in the SCTP dissector in Wireshark 1.8.x before 1.8.4 allows remote attackers to cause a denial of service (infinite loop) via a crafted Duplicate TSN count.

CVE-2012-6056 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
openSUSE-SU-2013:0151-1: moderate: wireshark to 1.8.4	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0151
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:0341
Wireshark · wnpa-sec-2012-33	Vendor Advisory www.wireshark.org text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2012-33.html
code.wireshark Code Review - wireshark.git/tree	Patch anonsvn.wireshark.org text/xml	CONFIRM anonsvn.wireshark.org/viewvc/trunk/epan/dissectors/packet-sctp.c? r1=45355&r2=45354&pathrev=45355
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=45355
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org/mitre.oval:def:16139
7802 – Buildbot crash output: fuzz-2012-10-06-8603.pcap	bugs.wireshark.org text/html	 CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=7802

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	1.8.0	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	1.8.0	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:1.8.0:*****:						
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:1.8.0:*****:						
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

© [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](#)