



CVE-2013-4927

Published on: 07/29/2013 12:00:00 AM UTC

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

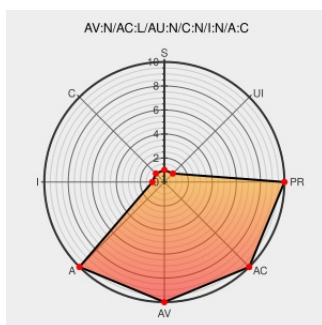
CVE-2013-4927

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

Integer signedness error in the `get_type_length` function in `epan/dissectors/packet-btsdp.c` in the Bluetooth SDP dissector in Wireshark 1.8.x before 1.8.9 and 1.10.x before 1.10.1 allows remote attackers to cause a denial of service (loop and CPU consumption) via a crafted packet.

CVE-2013-4927 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Red Hat Customer Portal

[web.archive.org](#)

[text/html](#)

Inactive Link Not Archived

[REDHAT RHSA-2014:0341](#)

openSUSE-SU-2013:1300-1: moderate:
wireshark to 1.8.9

[lists.opensuse.org](#)

[text/html](#)

[SUSE openSUSE-SU-2013:1300](#)

Security Advisory SA54371 - SUSE update for
wireshark - Secunia

[web.archive.org](#)

[text/html](#)

[SECUNIA 54371](#)

Wireshark · Wireshark 1.8.9 Release Notes

[www.wireshark.org](#)

[text/html](#)

[CONFIRM www.wireshark.org/docs/relnotes/wireshark-1.8.9.html](#)

Wireshark · wnpa-sec-2013-45 · Bluetooth SDP
dissector large loop

[Vendor Advisory](#)

[www.wireshark.org](#)

[CONFIRM www.wireshark.org/security/wnpa-sec-2013-45.html](#)

	text/html	
code.wireshark Code Review - wireshark.git/tree	Patch anonsvn.wireshark.org text/xml	CONFIRM anonsvn.wireshark.org/viewvc?view=revision&revision=50134
8831 – BTSDP dissector hangs	bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=8831
Security Advisory SA54425 - Gentoo update for wireshark - Secunia	web.archive.org text/html	SECUNIA 54425
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:17636
Gentoo Linux Documentation -- Wireshark: Multiple vulnerabilities	www.gentoo.org text/html	GENTOO GLSA-201308-05
Security Advisory SA54296 - Wireshark Multiple Denial of Service Vulnerabilities - Secunia	web.archive.org text/html	SECUNIA 54296
openSUSE-SU-2013:1295-1: moderate: wireshark to 1.8.9	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1295
Wireshark · Wireshark 1.10.1 Release Notes	www.wireshark.org text/html	CONFIRM www.wireshark.org/docs/relnotes/wireshark-1.10.1.html
code.wireshark Code Review - wireshark.git/tree	Patch anonsvn.wireshark.org text/xml	CONFIRM anonsvn.wireshark.org/viewvc/trunk/epan/dissectors/packet-btsdp.c?r1=50134&r2=50133&pathrev=50134

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	1.8.0	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	1.8.4	All	All	All
Application	Wireshark	Wireshark	1.8.5	All	All	All
Application	Wireshark	Wireshark	1.8.6	All	All	All
Application	Wireshark	Wireshark	1.8.7	All	All	All
Application	Wireshark	Wireshark	1.8.8	All	All	All
Application	Wireshark	Wireshark	1.10.0	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	1.8.4	All	All	All
Application	Wireshark	Wireshark	1.8.5	All	All	All
Application	Wireshark	Wireshark	1.8.6	All	All	All
Application	Wireshark	Wireshark	1.8.7	All	All	All
Application	Wireshark	Wireshark	1.8.8	All	All	All

cpe:2.3:a:wireshark:wireshark:1.10.0:****:*:*:*:
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:1.8.4:****:*:*:*:
cpe:2.3:a:wireshark:wireshark:1.8.5:****:*:*:*:
cpe:2.3:a:wireshark:wireshark:1.8.6:****:*:*:*:
cpe:2.3:a:wireshark:wireshark:1.8.7:****:*:*:*:
cpe:2.3:a:wireshark:wireshark:1.8.8:****:*:*:*:
cpe:2.3:a:wireshark:wireshark:1.10.0:****:*:*:*:
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:1.8.4:****:*:*:*:
cpe:2.3:a:wireshark:wireshark:1.8.5:****:*:*:*:
cpe:2.3:a:wireshark:wireshark:1.8.6:****:*:*:*:
cpe:2.3:a:wireshark:wireshark:1.8.7:****:*:*:*:
cpe:2.3:a:wireshark:wireshark:1.8.8:****:*:*:*:

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](#)