



CVE-2013-4935

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

Last Modified on: 03/23/2021 11:28:29 PM UTC

CVE-2013-4935

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

The dissect_per_length_determinant function in epan/dissectors/packet-per.c in the ASN.1 PER dissector in Wireshark 1.8.x before 1.8.9 and 1.10.x before 1.10.1 does not initialize a length field in certain abnormal situations, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.

CVE-2013-4935 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

NONE

PARTIAL

CVE References

Description

Tags

Link

8722 – ASN.1 aligned PER dissector fails to check return value of g_malloc()

[bugs.wireshark.org](#)
[text/html](#)

CONFIRM [bugs.wireshark.org/bugzilla/show_bug.cgi?id=8722](#)

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

code.wireshark Code Review - wireshark.git/tree

[Patch](#)
[anonsvn.wireshark.org](#)
[text/xml](#)

CONFIRM
[anonsvn.wireshark.org/viewvc/trunk/epan/dissectors/packet-per.c?r1=49985&r2=49984&pathrev=49985](#)

Security Advisory SA54371 - SUSE update for

[web.archive.org](#)

SECUNIA 54371

wireshark - Secunia	text/html	
Wireshark · Wireshark 1.8.9 Release Notes	www.wireshark.org text/html	 CONFIRM www.wireshark.org/docs/relnotes/wireshark-1.8.9.html
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:17417
Security Advisory SA54425 - Gentoo update for wireshark - Secunia	web.archive.org text/html	 SECUNIA 54425
Wireshark · wnpa-sec-2013-52 · ASN.1 PER dissector crash	Vendor Advisory www.wireshark.org text/html	 CONFIRM www.wireshark.org/security/wnpa-sec-2013-52.html
Debian -- Security Information -- DSA-2734-1 wireshark	www.debian.org Deprecated Link text/html	 DEBIAN DSA-2734
code.wireshark Code Review - wireshark.git/tree	Patch anonsvn.wireshark.org text/xml	 CONFIRM anonsvn.wireshark.org/viewvc?view=revision&revision=49985
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
Security Advisory SA54178 - Debian update for wireshark - Secunia	web.archive.org text/html	 SECUNIA 54178
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

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

[← 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](#)