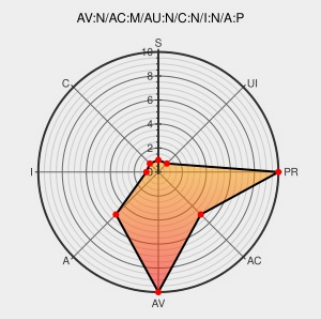
CVE-2012-0041

Published on: 04/11/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:14 AM UTC

CVE-2012-0041

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Enterprise Linux from Redhat contain the following vulnerability:

The dissect_packet function in epan/packet.c in Wireshark 1.4.x before 1.4.11 and 1.6.x before 1.6.5 allows remote attackers to cause a denial of service (application crash) via a long packet in a capture file, as demonstrated by an airopeek file.

CVE-2012-0041 has been assigned by secalert@redhat.com 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
oss-security - Re: CVE request: Wireshark multiple vulnerabilities	www.openwall.com, text/html	MLIST [oss-security] 20120111 Re: CVE request: Wireshark multiple vulnerabilities
Security Alerts - Secunia	web.archive.org, text/html	SECUNIA 48947
Red Hat Customer Portal	web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2013:0125
code.wireshark Code Review - wireshark.git/tree	Patch, anonsvn.wireshark.org, text/xml	CONFIRM anonsvn.wireshark.org/viewvc?view=revision&revision=40164
Repository / Oval Repository	oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:15297

Security Advisory SA54425 - Gentoo update for wireshark - Secunia	web.archive.org text/html	SECUNIA 54425
oss-security - Re: CVE request: Wireshark multiple vulnerabilities	www.openwall.com text/html	MLIST [oss-security] 20120119 Re: CVE request: Wireshark multiple vulnerabilities
6663 – Large packet length crashes Wireshark	Exploit Patch bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=6663
Wireshark · wnpa-sec-2012-01	Vendor Advisory www.wireshark.org text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2012-01.html
Gentoo Linux Documentation -- Wireshark: Multiple vulnerabilities	www.gentoo.org text/html	GENTOO GLSA-201308-05
Security Alerts - Secunia	web.archive.org text/html	SECUNIA 47494

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
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Application	Wireshark	Wireshark	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.10	All	All	All
Application	Wireshark	Wireshark	1.4.2	All	All	All
Application	Wireshark	Wireshark	1.4.3	All	All	All
Application	Wireshark	Wireshark	1.4.4	All	All	All
Application	Wireshark	Wireshark	1.4.5	All	All	All
Application	Wireshark	Wireshark	1.4.6	All	All	All
Application	Wireshark	Wireshark	1.4.7	All	All	All
Application	Wireshark	Wireshark	1.4.8	All	All	All
Application	Wireshark	Wireshark	1.4.9	All	All	All
Application	Wireshark	Wireshark	1.6.0	All	All	All
Application	Wireshark	Wireshark	1.6.1	All	All	All
Application	Wireshark	Wireshark	1.6.2	All	All	All

Application	Wireshark	Wireshark	1.6.3	All	All	All
Application	Wireshark	Wireshark	1.6.4	All	All	All
Application	Wireshark	Wireshark	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.10	All	All	All
Application	Wireshark	Wireshark	1.4.2	All	All	All
Application	Wireshark	Wireshark	1.4.3	All	All	All
Application	Wireshark	Wireshark	1.4.4	All	All	All
Application	Wireshark	Wireshark	1.4.5	All	All	All
Application	Wireshark	Wireshark	1.4.6	All	All	All
Application	Wireshark	Wireshark	1.4.7	All	All	All
Application	Wireshark	Wireshark	1.4.8	All	All	All
Application	Wireshark	Wireshark	1.4.9	All	All	All
Application	Wireshark	Wireshark	1.6.0	All	All	All
Application	Wireshark	Wireshark	1.6.1	All	All	All
Application	Wireshark	Wireshark	1.6.2	All	All	All
Application	Wireshark	Wireshark	1.6.3	All	All	All
Application	Wireshark	Wireshark	1.6.4	All	All	All

cpe:2.3:o:redhat:enterprise_linux:5:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:5:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.10:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.4:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.5:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.6:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.7:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.8:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.9:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.6.1:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.2:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.3:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.4:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.4.0:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.4.1:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.4.10:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.4.2:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.4.3:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.4.4:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.4.5:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.4.6:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.4.7:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.4.8:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.4.9:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.0:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.1:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.2:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.3:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.4:*:*:*:*:*:*:*

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 registred 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