



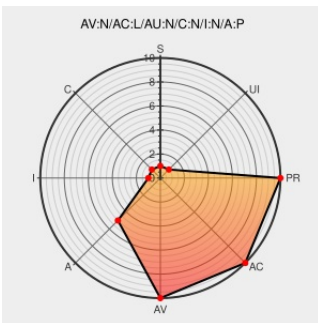
Last Modified on: 03/23/2021 11:28:44 PM UTC

CVE-2003-1013

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

The Q.931 dissector in *Ethereal* before 0.10.0, and *Tethereal*, allows remote attackers to cause a denial of service (crash) via a malformed Q.931, which triggers a null dereference.

CVE-2003-1013 has been assigned by  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
Secunia - Advisories - Debian update for ethereal	web.archive.org text/html	 SECUNIA 10531
No Description Provided	patches.sgi.com Inactive Link Not Archived	 SGI 20040103-01-U
redhat.com Red Hat Support	Patch Vendor Advisory www.redhat.com text/html	 REDHAT RHSA-2004:001
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:857
Ethereal: enpa-sa-00012	Patch Vendor Advisory	 CONFIRM www.ethereal.com/apnotes/enpa-sa-00012.html

	www.ethereal.com text/html	
Debian -- Page not found	www.debian.org Deprecated Link text/html Inactive Link Not Archived	 DEBIAN DSA-407
Secunia - Advisories - Red Hat update for Ethereal	web.archive.org text/html	 SECUNIA 10570
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:10097
Mandriva Security Advisories	www.mandriva.com text/html	 MANDRAKE MDKSA-2004:002
Home - Conectiva	distro.conectiva.com.br text/html	 CONECTIVA CLA-2004:801
No Description Provided	patches.sgi.com Inactive Link Not Archived	 SGI 20040202-01-U
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2004:002
Secunia - Advisories - Conectiva update for ethereal	web.archive.org text/html	 SECUNIA 10568
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	Ethereal Group	Ethereal	0.9	All	All	All
Application	Ethereal Group	Ethereal	0.9.1	All	All	All
Application	Ethereal Group	Ethereal	0.9.10	All	All	All
Application	Ethereal Group	Ethereal	0.9.11	All	All	All
Application	Ethereal Group	Ethereal	0.9.12	All	All	All
Application	Ethereal Group	Ethereal	0.9.13	All	All	All
Application	Ethereal Group	Ethereal	0.9.14	All	All	All
Application	Ethereal Group	Ethereal	0.9.15	All	All	All
Application	Ethereal Group	Ethereal	0.9.16	All	All	All
Application	Ethereal Group	Ethereal	0.9.2	All	All	All
Application	Ethereal Group	Ethereal	0.9.3	All	All	All
Application	Ethereal Group	Ethereal	0.9.4	All	All	All

Application	Ethereal Group	Ethereal	0.9.5	All	All	All
Application	Ethereal Group	Ethereal	0.9.6	All	All	All
Application	Ethereal Group	Ethereal	0.9.7	All	All	All
Application	Ethereal Group	Ethereal	0.9.8	All	All	All
Application	Ethereal Group	Ethereal	0.9.9	All	All	All
Application	Ethereal Group	Ethereal	0.9	All	All	All
Application	Ethereal Group	Ethereal	0.9.1	All	All	All
Application	Ethereal Group	Ethereal	0.9.10	All	All	All
Application	Ethereal Group	Ethereal	0.9.11	All	All	All
Application	Ethereal Group	Ethereal	0.9.12	All	All	All
Application	Ethereal Group	Ethereal	0.9.13	All	All	All
Application	Ethereal Group	Ethereal	0.9.14	All	All	All
Application	Ethereal Group	Ethereal	0.9.15	All	All	All
Application	Ethereal Group	Ethereal	0.9.16	All	All	All
Application	Ethereal Group	Ethereal	0.9.2	All	All	All
Application	Ethereal Group	Ethereal	0.9.3	All	All	All
Application	Ethereal Group	Ethereal	0.9.4	All	All	All
Application	Ethereal Group	Ethereal	0.9.5	All	All	All
Application	Ethereal Group	Ethereal	0.9.6	All	All	All
Application	Ethereal Group	Ethereal	0.9.7	All	All	All
Application	Ethereal Group	Ethereal	0.9.8	All	All	All
Application	Ethereal Group	Ethereal	0.9.9	All	All	All
cpe:2.3:a:ethereal_group:ethereal:0.9:*:*:*:*:*.*:						
cpe:2.3:a:ethereal_group:ethereal:0.9.1:*:*:*:*:*.*:						
cpe:2.3:a:ethereal_group:ethereal:0.9.10:*:*:*:*:*.*:						
cpe:2.3:a:ethereal_group:ethereal:0.9.11:*:*:*:*:*.*:						
cpe:2.3:a:ethereal_group:ethereal:0.9.12:*:*:*:*:*.*:						
cpe:2.3:a:ethereal_group:ethereal:0.9.13:*:*:*:*:*.*:						
cpe:2.3:a:ethereal_group:ethereal:0.9.14:*:*:*:*:*.*:						
cpe:2.3:a:ethereal_group:ethereal:0.9.15:*:*:*:*:*.*:						
cpe:2.3:a:ethereal_group:ethereal:0.9.16:*:*:*:*:*.*:						
cpe:2.3:a:ethereal_group:ethereal:0.9.2:*:*:*:*:*.*:						
cpe:2.3:a:ethereal_group:ethereal:0.9.3:*:*:*:*:*.*:						

cpe:2.3:a:ethereum_group:ethereum:0.9.4:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.5:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.6:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.7:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.8:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.9:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.1:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.10:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.11:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.12:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.13:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.14:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.15:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.16:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.2:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.3:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.4:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.5:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.6:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.7:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.8:*****:
cpe:2.3:a:ethereum_group:ethereum:0.9.9:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)