

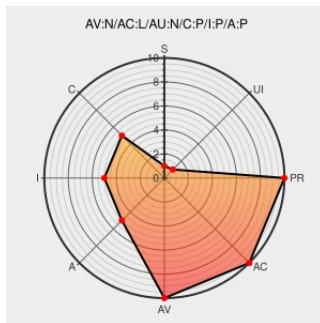


CVE-2005-1461

Published on: 05/05/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:25 AM UTC

CVE-2005-1461

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

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

Multiple buffer overflows in the (1) SIP, (2) CMIP, (3) CMP, (4) CMS, (5) CRMF, (6) ESS, (7) OCSP, (8) X.509, (9) ISIS, (10) DISTCC, (11) FCELS, (12) Q.931, (13) NCP, (14) TCAP, (15) ISUP, (16) MEGACO, (17) PKIX1Explitt, (18) PKIX_Qualified, (19) Presentation dissectors in Ethereal before 0.10.11 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code.

CVE-2005-1461 has been assigned by [secalert@redhat.com](#) to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

[rhn.redhat.com](#) | Red Hat Support

[www.redhat.com](#)
text/html

[REDHAT RHSA-2005:427](#)

[Ethereal: enpa-sa-00019](#)

[www.ethereal.com](#)
text/xml

[CONFIRM www.ethereal.com/appnotes/enpa-sa-00019.html](#)

[Home - Conectiva](#)

[distro.conectiva.com.br](#)
text/html

[CONECTIVA CLSA-2005:963](#)

[Repository / Oval Repository](#)

[oval.cisecurity.org](#)
text/html

[OVAL oval.org.mitre.oval:def:9853](#)

[Ethereal: News Article](#)

[www.ethereal.com](#)
text/xml

[CONFIRM www.ethereal.com/news/item_20050504_01.html](#)

[FLSA-2006:152922] Updated ethereal packages fix security issues

www.redhat.com
[text/html](#)

 **FEDORA** FLSA-2006:152922

Ethereal Multiple Remote Protocol Dissector Vulnerabilities

[cve.report \(archive\)](#)
[text/html](#)

 **BID 13504**

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	0.10	All	All	All
Application	Ethereal Group	Ethereal	0.10.0	All	All	All
Application	Ethereal Group	Ethereal	0.10.1	All	All	All
Application	Ethereal Group	Ethereal	0.10.10	All	All	All
Application	Ethereal Group	Ethereal	0.10.2	All	All	All
Application	Ethereal Group	Ethereal	0.10.3	All	All	All
Application	Ethereal Group	Ethereal	0.10.4	All	All	All
Application	Ethereal Group	Ethereal	0.10.5	All	All	All
Application	Ethereal Group	Ethereal	0.10.6	All	All	All
Application	Ethereal Group	Ethereal	0.10.7	All	All	All
Application	Ethereal Group	Ethereal	0.10.8	All	All	All
Application	Ethereal Group	Ethereal	0.10.9	All	All	All
Application	Ethereal Group	Ethereal	0.8	All	All	All
Application	Ethereal Group	Ethereal	0.8.13	All	All	All
Application	Ethereal Group	Ethereal	0.8.14	All	All	All
Application	Ethereal Group	Ethereal	0.8.15	All	All	All
Application	Ethereal Group	Ethereal	0.8.18	All	All	All
Application	Ethereal Group	Ethereal	0.8.19	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

[illegible]

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:0.10:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.10.0:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.10.1:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.10.10:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.10.2:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.10.3:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.10.4:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.10.5:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.10.6:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.10.7:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.10.8:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.10.9:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.8:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.8.13:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.8.14:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.8.15:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.8.18:*****:***:						
cpe:2.3:a:ethereal_group:ethereal:0.8.19:*****:***:						
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:ethereal_group:ethereal:0.9.4:*****:
cpe:2.3:a:ethereal_group:ethereal:0.9.5:*****:
cpe:2.3:a:ethereal_group:ethereal:0.9.6:*****:
cpe:2.3:a:ethereal_group:ethereal:0.9.7:*****:
cpe:2.3:a:ethereal_group:ethereal:0.9.8:*****:
cpe:2.3:a:ethereal_group:ethereal:0.9.9:*****:
cpe:2.3:a:ethereal_group:ethereal:0.10:*****:
cpe:2.3:a:ethereal_group:ethereal:0.10.0:*****:
cpe:2.3:a:ethereal_group:ethereal:0.10.1:*****:
cpe:2.3:a:ethereal_group:ethereal:0.10.10:*****:
cpe:2.3:a:ethereal_group:ethereal:0.10.2:*****:
cpe:2.3:a:ethereal_group:ethereal:0.10.3:*****:
cpe:2.3:a:ethereal_group:ethereal:0.10.4:*****:
cpe:2.3:a:ethereal_group:ethereal:0.10.5:*****:
cpe:2.3:a:ethereal_group:ethereal:0.10.6:*****:
cpe:2.3:a:ethereal_group:ethereal:0.10.7:*****:
cpe:2.3:a:ethereal_group:ethereal:0.10.8:*****:
cpe:2.3:a:ethereal_group:ethereal:0.10.9:*****:
cpe:2.3:a:ethereal_group:ethereal:0.8:*****:

cpe:2.3:a:ethereal_group:ethereal:0.8.13:*****:
cpe:2.3:a:ethereal_group:ethereal:0.8.14:*****:
cpe:2.3:a:ethereal_group:ethereal:0.8.15:*****:
cpe:2.3:a:ethereal_group:ethereal:0.8.18:*****:
cpe:2.3:a:ethereal_group:ethereal:0.8.19:*****:
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:ethereal_group:ethereal:0.9.4:*****:
cpe:2.3:a:ethereal_group:ethereal:0.9.5:*****:
cpe:2.3:a:ethereal_group:ethereal:0.9.6:*****:
cpe:2.3:a:ethereal_group:ethereal:0.9.7:*****:
cpe:2.3:a:ethereal_group:ethereal:0.9.8:*****:
cpe:2.3:a:ethereal_group:ethereal:0.9.9:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)