

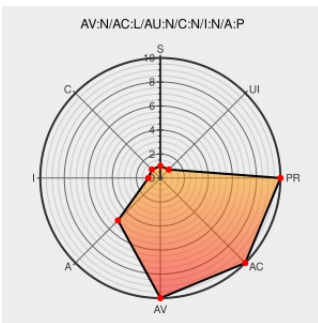


CVE-2005-2361

Published on: 08/10/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:26 AM UTC

CVE-2005-2361

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

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

Unknown vulnerability in the (1) AgentX dissector, (2) PER dissector, (3) DOCSIS dissector, (4) SCTP graphs, (5) HTTP dissector, (6) DCERPC, (7) DHCP, (8) RADIUS dissector, (9) Telnet dissector, (10) IS-IS LSP dissector, or (11) NCP dissector in Ethereal 0.8.19 through 0.10.11 allows remote attackers to cause a denial of service

(application crash or abort) via unknown attack vectors.

CVE-2005-2361 has been assigned by secalert@redhat.com 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	X SECUNIA 17102
Secunia - Advisories - Ethereal Multiple Protocol Dissector and zlib Vulnerabilities	web.archive.org text/html	X SECUNIA 16225
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval.org.mitre.oval:def:10225
Gentoo Linux Documentation -- Ethereal: Multiple vulnerabilities	Patch www.gentoo.org text/html	GENTOO GLSA-200507-27
Ethereal Multiple Protocol Dissector Vulnerabilities	cve.report (archive)	GID BID 14399

	text/html	
Debian -- Security Information -- DSA-853-1 ethereal	www.debian.org Depreciated Link text/html	 DEBIAN DSA-853
[FLSA-2006:152922] Updated ethereal packages fix security issues	www.redhat.com text/html	 FEDORA FLSA-2006:152922
Ethereal: enpa-sa-00020	Patch www.ethereal.com text/xml	 CONFIRM www.ethereal.com/appnotes/enpa-sa-00020.html
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2005:687
Security Announcement	web.archive.org text/html Inactive Link Not Archived	 SUSE SUSE-SR:2005:019
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	0.10.0	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	0.10.11	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	0.8.19	All	All	All
Application	Ethereal Group	Ethereal	0.8.20	All	All	All
Application	Ethereal Group	Ethereal	0.9.0	All	All	All
Application	Ethereal Group	Ethereal	0.9.1	All	All	All
Application	Ethereal Group	Ethereal	0.9.10	All	All	All

[illegible]

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:0.10.0:*****:						
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:0.10.11:*****:						
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:0.8.19:*****:						
cpe:2.3:a:ethereal_group:ethereal:0.8.20:*****:						
cpe:2.3:a:ethereal_group:ethereal:0.9.0:*****:						
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:0.10.0:*****:
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:0.10.11:*****:
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:0.8.19:*****:
cpe:2.3:a:ethereal_group:ethereal:0.8.20:*****:
cpe:2.3:a:ethereal_group:ethereal:0.9.0:*****:
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 →](#)