



CVE-2005-3242

Published on: 10/27/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:42 AM UTC

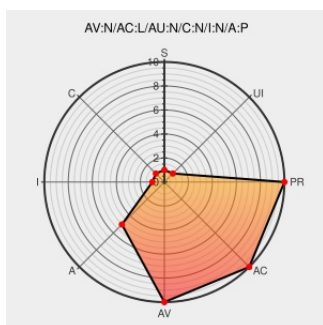
CVE-2005-3242

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Ethereal 0.10.12 and earlier allows remote attackers to cause a denial of service (crash) via unknown vectors in (1) the IrDA dissector and (2) the SMB dissector when SMB transaction payload reassembly is enabled.

CVE-2005-3242 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Secunia - Advisories - Gentoo update for ethereal

[web.archive.org](#)
[text/html](#)

[SECUNIA 17377](#)

Secunia - Advisories - Red Hat update for ethereal

[web.archive.org](#)
[text/html](#)

[SECUNIA 17327](#)

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

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

[REDHAT RHSA-2005:809](#)

Debian -- Security Information -- DSA-1171-1 ethereal

[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

[DEBIAN DSA-1171](#)

Security Announcement

[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[SUSE SUSE-SR:2005:025](#)

Secunia - Advisories - Ethereum Multiple Protocol Dissector and PCRE Vulnerabilities	web.archive.org text/html	 SECUNIA 17254
Secunia - Advisories - Avaya Multiple Ethereum Vulnerabilities	web.archive.org text/html	 SECUNIA 17392
Ethereal: enpa-sa-00021	Patch www.ethereal.com text/xml	 CONFIRM www.ethereal.com/appnotes/enpa-sa-00021.html
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 20133
Gentoo Linux Documentation -- Ethereum: Multiple vulnerabilities in protocol dissectors	www.gentoo.org text/html	 GENTOO GLSA-200510-25
Debian update for ethereal - Advisories - Secunia	web.archive.org text/html	 SECUNIA 21813
[FLSA-2006:152922] Updated ethereal packages fix security issues	www.redhat.com text/html	 FEDORA FLSA-2006:152922
SecurityTracker.com Archives - Ethereum Bugs in Multiple Dissectors Let Remote Users Execute Arbitrary Code or Cause Denial of Service Conditions	securitytracker.com text/html	 SECTRAK 1015082
Ethereal Multiple Protocol Dissector Vulnerabilities In Versions Prior To 0.10.13	cve.report (archive) text/html	 BID 15148
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 20125
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:10558
Secunia - Advisories - SUSE Updates for Multiple Packages	web.archive.org text/html	 SECUNIA 17480
Secunia - Advisories - Fedora update for ethereal	web.archive.org text/html	 SECUNIA 17286

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	0.10.12	All	All	All
Application	Ethereal Group	Ethereal	0.10.2	All	All	All

[illegible]

Application	Ethereal Group	Ethereal	0.9.15	All	All	All
Application	Ethereal Group	Ethereal	0.9.16	All	All	All
Application	Ethereal Group	Ethereal	0.9.7	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:0.10.12:*****:						
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:0.9.10:*****:						
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:0.9.7:*****:						
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:0.10.12:*****:
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:0.9.10:*****:
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:0.9.7:*****:
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](#)