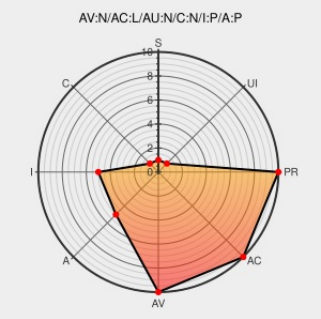
CVE-2005-3249

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

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

CVE-2005-3249

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



Certain versions of Ethereal from Ethereal Group contain the following vulnerability:

Unspecified vulnerability in the WSP dissector in Ethereal 0.10.1 to 0.10.12 allows remote attackers to cause a denial of service or corrupt memory via unknown vectors that cause Ethereal to free an invalid pointer.

CVE-2005-3249 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	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
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SR:2005:025
Secunia - Advisories - Ethereal Multiple Protocol Dissector and PCRE Vulnerabilities	web.archive.org text/html	SECUNIA 17254
Secunia - Advisories - Avaya Multiple Ethereal Vulnerabilities	web.archive.org	SECUNIA 17392

	text/html	
Ethereal: enpa-sa-00021	Vendor Advisory www.ethereal.com text/xml	CONFIRM www.ethereal.com/appnotes/enpa-sa-00021.html
Gentoo Linux Documentation -- Ethereal: Multiple vulnerabilities in protocol dissectors	www.gentoo.org text/html	GENTOO GLSA-200510-25
[FLSA-2006:152922] Updated ethereal packages fix security issues	www.redhat.com text/html	FEDORA FLSA-2006:152922
SecurityTracker.com Archives - Ethereal Bugs in Multiple Dissectors Let Remote Users Execute Arbitrary Code or Cause Denial of Service Conditions	securitytracker.com text/html	SECTRACK 1015082
Ethereal Multiple Protocol Dissector Vulnerabilities In Versions Prior To 0.10.13	cve.report (archive) text/html	BID 15148
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:9313
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 20136
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

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	0.10.1	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
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	0.10.1	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
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

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:0.10.1:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→