

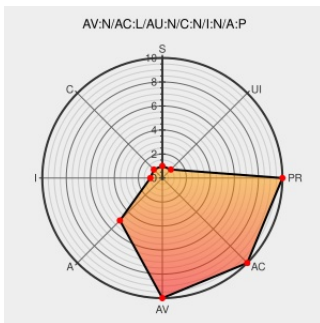


CVE-2004-0506

Published on: 06/03/2004 12:00:00 AM UTC

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

CVE-2004-0506

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

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

The SPNEGO dissector in Ethereal 0.9.8 to 0.10.3 allows remote attackers to cause a denial of service (crash) via unknown attack vectors that cause a null pointer dereference.

CVE-2004-0506 has been assigned by [M](#) cve@mitre.org 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

Ethereal Multiple Protocol Dissector Vulnerabilities

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

[🌐](#) [BID 10347](#)

Secunia - Advisories - Ethereal Multiple Vulnerabilities

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

[X](#) [SECUNIA 11608](#)

SecurityTracker.com Archives - Ethereal SIP, AIM, SPNEGO, and MMSE Dissector Flaws Allow Remote Users to Crash Ethereal or Execute Arbitrary Code

[securitytracker.com](#)
[text/html](#)

[🌐](#) [SECTRAK 1010158](#)

Ethereal: enpa-sa-00014

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

[e](#) [CONFIRM](#)
[www.ethereal.com/appnotes/enpa-sa-00014.html](#)

No Description Provided

[patches.sgi.com](#)

[🌐](#) [SGI 20040604-01-U](#)

	Inactive Link Not Archived	
No Description Provided	patches.sgi.com	 SGI 20040605-01-U
	Inactive Link Not Archived	
Secunia - Advisories - Red Hat update for ethereal	web.archive.org text/html	 SECUNIA 11836
Home - Conectiva	distro.conectiva.com.br text/html	 CONECTIVA CLA-2005:916
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:9695
Secunia - Advisories - Gentoo update for ethereal	web.archive.org text/html	 SECUNIA 11776
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:987
Gentoo Linux Documentation -- Ethereal: Multiple security problems	Vendor Advisory security.gentoo.org text/html	 GENTOO GLSA-200406-01
O-150: Multiple Security Problems in Ethereal 0.10.3	web.archive.org text/html Inactive Link Not Archived	 CIAC O-150
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF ethereal-spnego-dos(16151)
redhat.com Red Hat Support	Patch Vendor Advisory www.redhat.com text/html	 REDHAT RHSA-2004:234

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	0.10.1	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	0.10.1	All	All	All
Application	Ethereal Group	Ethereal	0.10.2	All	All	All
Application	Ethereal Group	Ethereal	0.10.3	All	All	All
Application	Sgi	Propack	2.4	All	All	All
Application	Sgi	Propack	3.0	All	All	All

Application	Sgi	Propack	2.4	All	All	All
Application	Sgi	Propack	3.0	All	All	All
cpe:2.3:a:ethereal_group:ethereal:0.10.1:*****:*.:						
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:0.10.1:*****:*.:						
cpe:2.3:a:ethereal_group:ethereal:0.10.2:*****:*.:						
cpe:2.3:a:ethereal_group:ethereal:0.10.3:*****:*.:						
cpe:2.3:a:sgi:propack:2.4:*****:*.:						
cpe:2.3:a:sgi:propack:3.0:*****:*.:						
cpe:2.3:a:sgi:propack:2.4:*****:*.:						
cpe:2.3:a:sgi:propack:3.0:*****:*.:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)