CVE-2004-0505

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2004-0505
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-08-18 04:00:00 UTC
Updated	2017-10-11 01:29:00 UTC
Description	The AIM dissector in Ethereal 0.10.3 allows remote attackers to cause a denial of service (assert error) via unknown attack

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
Ethereal Multiple Protocol Dissector Vulnerabilities
Secunia - Advisories - Ethereal Multiple Vulnerabilities
SecurityTracker.com Archives - Ethereal SIP, AIM, SPNEGO, and MMSE Dissector Flaws Allow Remote Users to Crash Ethereal or Execute
Repository / Oval Repository

IBM X-Force Exchange
Ethereal: enpa-sa-00014
20040604-01-U
20040605-01-U
6132
Secunia - Advisories - Red Hat update for ethereal
Home - Conectiva
Secunia - Advisories - Gentoo update for ethereal
Gentoo Linux Documentation -- Ethereal: Multiple security problems
O-150: Multiple Security Problems in Ethereal 0.10.3
Repository / Oval Repository
redhat.com | Red Hat Support
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**