CVE-2004-0504

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

Summary

CVE	CVE-2004-0504
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-08-18 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Ethereal 0.10.3 allows remote attackers to cause a denial of service (crash) via certain SIP messages between Hotsip serv

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

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	Sgi	Propack	2.4	All	All	All
Application	Sgi	Propack	3.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
SecurityTracker.com Archives - Ethereal SIP, AIM, SPNEGO, and MMSE Dissector Flaws Allow Remote Users to Crash Ethereal or Execute
Repository / Oval Repository
patches.sgi.com/support/free/security/advisories/20040605-01-U.asc
Secunia - Advisories - Ethereal Multiple Vulnerabilities
Home - Conectiva
Gentoo Linux Documentation -- Ethereal: Multiple security problems
redhat.com | Red Hat Support
Ethereal Multiple Protocol Dissector Vulnerabilities
Ethereal: enpa-sa-00014
Secunia - Advisories - Red Hat update for ethereal
patches.sgi.com/support/free/security/advisories/20040604-01-U.asc
Repository / Oval Repository
www.osvdb.org/6131
IBM X-Force Exchange
O-150: Multiple Security Problems in Ethereal 0.10.3
Ethereal: Re: [Ethereal-users] HotSIP sip-messages crasching ethereal
Secunia - Advisories - Gentoo update for ethereal
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.