



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 - Ethereum SIP, AIM, SPNEGO, and MMSE Dissector Flaws Allow Remote Users to Crash Ethereum or Execute Arbitrary Code
Repository / Oval Repository
patches.sgi.com/support/free/security/advisories/20040605-01-U.asc
Secunia - Advisories - Ethereum Multiple Vulnerabilities
Home - Conectiva
Gentoo Linux Documentation -- Ethereum: Multiple security problems
redhat.com Red Hat Support
Ethereum Multiple Protocol Dissector Vulnerabilities
Ethereum: enpa-sa-00014
Secunia - Advisories - Red Hat update for ethereum
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 Ethereum 0.10.3
Ethereum: Re: [Ethereum-users] HotSIP sip-messages crashing ethereum
Secunia - Advisories - Gentoo update for ethereum
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.

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#).

Free CVE JSON API cve.report/api

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