

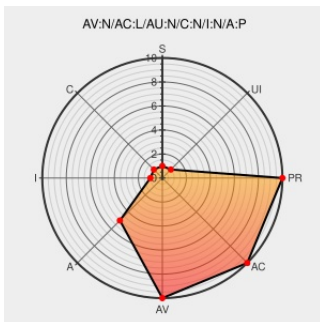


CVE-2002-1485

Published on: 03/18/2003 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:01 PM UTC

CVE-2002-1485

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

Certain versions of [Trillian](#) from [Cerulean Studios](#) contain the following vulnerability:

The AIM component of Trillian 0.73 and 0.74 allows remote attackers to cause a denial of service (crash) via certain strings such as "P > O < C".

CVE-2002-1485 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

PARTIAL

CVE References

Description

Tags

Link

Trillian AIM Remote Denial Of Service Attack

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

[🌐](#) [BID 5783](#)

Neohapsis Archives - Bugtraq - Trillian Remote DoS Attack - AIM - From spikeman_at_computersecuritynow.com

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[🌐](#) [BUGTRAQ 20020923](#)
[Trillian Remote DoS Attack - AIM](#)

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	Cerulean Studios	Trillian	0.73	All	All	All
Application	Cerulean Studios	Trillian	0.74	All	All	All
Application	Cerulean Studios	Trillian	0.73	All	All	All
Application	Cerulean Studios	Trillian	0.74	All	All	All
cpe:2.3:a:cerulean_studios:trillian:0.73:*****:						
cpe:2.3:a:cerulean_studios:trillian:0.74:*****:						
cpe:2.3:a:cerulean_studios:trillian:0.73:*****:						
cpe:2.3:a:cerulean_studios:trillian:0.74:*****:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→