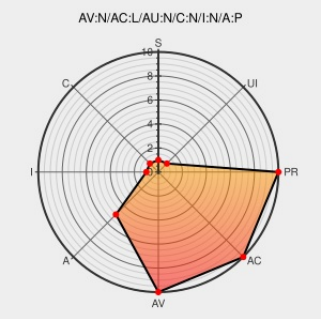
CVE-2003-0520

Published on: 07/10/2003 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:46 PM UTC

CVE-2003-0520

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Trillian from Cerulean Studios contain the following vulnerability:

Trillian 1.0 Pro and 0.74 Freeware allows remote attackers to cause a denial of service (crash) via a TypingUser message in which the "TypingUser" string has been modified.

CVE-2003-0520 has been assigned by 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
Cerulean Studios Trillian Client Malformed TypingUser Denial Of Service Vulnerability	Vendor Advisory, cve.report (archive), text/html	BID 8107
'Trillian Remote DoS' - MARC	marc.info, text/html	BUGTRAQ 20030704 Trillian Remote DoS

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	0.74	All	All	All
Application	Cerulean Studios	Trillian	1.0	All	All	All
Application	Cerulean Studios	Trillian	0.74	All	All	All
Application	Cerulean Studios	Trillian	1.0	All	All	All

cpe:2.3:a:cerulean_studios:trillian:0.74:*:*:*:*:*:*:*:

cpe:2.3:a:cerulean_studios:trillian:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:cerulean_studios:trillian:0.74:*:*:*:*:*:*:*:

cpe:2.3:a:cerulean_studios:trillian:1.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→