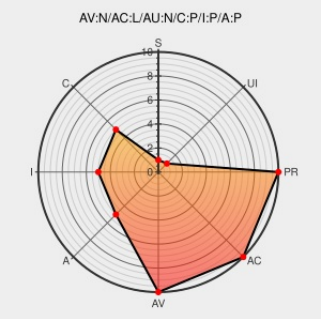
CVE-2002-1486

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

Last Modified on: 03/23/2021 11:26:02 PM UTC

CVE-2002-1486

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



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

Multiple buffer overflows in the IRC component of Trillian 0.73 and 0.74 allows remote malicious IRC servers to cause a denial of service and possibly execute arbitrary code via (1) a large response from the server, (2) a JOIN with a long channel name, (3) a long "raw 221" message, (4) a PRIVMSG with a long nickname, or (5) a long response from an IDENT server.

CVE-2002-1486 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Neohapsis Archives - Bugtraq - And Again. Trillian 'raw 221' Overflow. - From fitzies_at_hotmail.com	archives.neohapsis.com, text/x-c, Inactive Link, Not Archived	BUGTRAQ 20020921 And Again. Trillian 'raw 221' Overflow.
ISS X-Force Database: trillian-raw221-bo (10151): Trillian raw 221 user mode buffer overflow	Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	XF trillian-raw221-bo(10151)
Neohapsis Archives - Bugtraq - Yet Another. Trillian 'JOIN' Overflow. - From fitzies_at_hotmail.com	Exploit, Patch, Vendor Advisory, archives.neohapsis.com	BUGTRAQ 20020920 Yet Another. Trillian 'JOIN' Overflow.

	text/x-c Inactive Link Not Archived	
ISS X-Force Database: trillian-irc-server-bo (10163): Trillian IRC server buffer overflow	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	XF trillian-irc-server-bo(10163)
ISS X-Force Database: trillian-irc-join-bo (10150): Trillian IRC JOIN buffer overflow	web.archive.org text/html Inactive Link Not Archived	XF trillian-irc-join-bo(10150)
Trillian IRC User Mode Numeric Remote Buffer Overflow Vulnerability	Exploit Vendor Advisory cve.report (archive) text/html	BID 5769
Neohapsis Archives - NTBugtraq - Trillian .73 & .74 "PRIVMSG" Overflow. - From fitzies_at_HOTMAIL.COM	archives.neohapsis.com text/x-c Inactive Link Not Archived	NTBUGTRAQ 20020919 Trillian .73 & .74 "PRIVMSG" Overflow.
Trillian IRC JOIN Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 5765
Neohapsis Archives - Bugtraq - *sigh* Trillian multiple DoS's flaws. - From fitzies_at_hotmail.com	archives.neohapsis.com text/x-c Inactive Link Not Archived	BUGTRAQ 20020922 *sigh* Trillian multiple DoS
Trillian IRC Oversized Data Block Buffer Overflow Vulnerability	Exploit Patch Vendor Advisory cve.report (archive) text/html	BID 5777
Neohapsis Archives - NTBugtraq - Trillian .74 and below, ident flaw. - From fitzies_at_HOTMAIL.COM	archives.neohapsis.com text/x-c Inactive Link Not Archived	NTBUGTRAQ 20020914 Trillian .74 and below, ident flaw.

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	0.725	All	All	All
Application	Cerulean Studios	Trillian	0.73	All	All	All
Application	Cerulean Studios	Trillian	0.74	All	All	All
Application	Cerulean Studios	Trillian	0.725	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:0.725:*:*:*:*:*:*:*:

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:0.725:*:*:*:*:*:*:*:

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→