

By: [Andrei Popa](#), Security and Search Engines Editor

[Trillian in Trouble, Security Patch Required](#)

Vulnerability found in the IM application

Trillian is an application installed on lots of computers around the world for the simple reason that it allows users to communicate on the most popular instant messaging networks with a single software instance. Imagine that you have friends on Google Talk, MSN Messenger, Yahoo Messenger and ICQ. Keeping four applications in the System Tray isn't quite the most convenient thing to do, so starting a single program that would provide all the functions of the four tools is the best solution. Yes, I know, there are several other similar applications out there, but today we're talking about Trillian and its security flaw. And because we're on the Trillian vulnerability subject, find out that SecurityFocus has reported an "overly long nickname remote DoS vulnerability" in Trillian which may allow an attacker crash somebody's IM instance. According to the advisory, the issue affects both [Trillian 3.1](#) and Trillian Pro 3.1, but other versions may be affected as well. "Trillian is prone to a remote denial-of-service vulnerability because it fails to sufficiently bounds-check user-supplied data. Few details regarding this vulnerability are available; we will update this BID when more information emerges. Exploiting this issue allows remote attackers to trigger denial-of-service conditions, denying further service to legitimate users," SecurityFocus wrote in the advisory. At this time, there's no security patch, fix or update available on the web so extra-care is recommended when using the Trillian versions mentioned above. Trillian was quite a popular application in the past but, Cerulean Studios are preparing a new version of the program, codename Astra, which is supposed to bring lots of new functions to its users. At this time, the new flavor is only available in alpha stages so only a limited number of users are able to test it.