

# [EXPL] Buffer Overflow Vulnerability In Trillian

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0012.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 03/07/05

To: list@securiteam.com

Date: 7 Mar 2005 10:26:47 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list - Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

## Buffer Overflow Vulnerability In Trillian

---

### SUMMARY

<<http://www.ceruleanstudios.com>> Trillian is a fully featured, stand-alone, skinnable chat client that supports AIM, ICQ, MSN, Yahoo Messenger, and IRC.

Trillian contains a buffer overflow vulnerability in the way it handles the PNG Images. Presented here is an exploit for this vulnerability

### DETAILS

Vulnerable Systems:

- \* Trillian 3.0 Basic

Exploit:

```
#####
# See-security Technologies ltd. #
# http://www.see-security.com #
# Trillian 3.0 PNG Image Processing Buffer overflow Exploit #
# Discovered and coded by: Tal zeltzer #
#####
```

```
import sys
```



