

[NT] Trillian Plug-ins Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0155.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/31/05

To: list@securiteam.com

Date: 31 Mar 2005 11:16:41 +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>

Trillian Plug-ins Buffer Overflow

SUMMARY

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

A buffer iteration overflow was found in Trillian when it tries to handle HTTP 1.1 response headers.

DETAILS

Vulnerable Systems:

- * Trillian version 2.0
- * Trillian version 3.0
- * Trillian version 3.1

Trillian Version 2.0:

The vulnerability can be demonstrated in Trillian 2.0 by setting up a netcat listener on port 80 and then pointing Trillian's proxy, RSS reader or anything else that connects to HTTP to the netcat listener.

After the client connects, piping a very long string followed by a carriage return will crash the client. Specially crafted input may result

Securiteam: [NT] Trillian Plug-ins Buffer Overflow

in malicious code being executed under the context of the user that Trillian is running as. This problem is compounded because the same vulnerable code appears to have been copied into several different components and locations.

Trillian Version 3.0:

In Trillian 3.0, many instances of the bug were fixed, but at least one has persisted in the Yahoo IM component. This mistake is probably due to the duplication of the code that caused the vulnerability mentioned above. Trillian 3.0 is compiled with the Buffer Security Check option in Visual C++ 7.1 (also known as stack canaries), which helps prevent the exploitation of stack-based overflows. Since this is a heap overflow, the security check does not appear to help.

Trillian Version 3.1:

In Trillian 3.1, the aforementioned Yahoo IM vulnerabilities have not been fixed. There are still two exploitable buffer iteration bugs. One is at offset 0x520296c6 and the other is at offset 0x5201a05f. A Trillian developer who has access to the symbols and source code should use these offsets to locate and fix these problems.

The buffer iteration bug and the fact that it was likely to be exploitable due to its operating on user-supplied data. You can see another example of the exploitable code by looking at location 0x10004464 in Trillian 2.0's rss.dll. The vulnerable source probably looks approximately like this:

```
while ((ch != '\n') && (bytes != 0))
{
int bytes = recv(socket, &ch, 1, ...);
*buf++ = ch;
}
```

The buffer will overflow if a long string with many characters is received before the newline character over this network connection.

Disclosure Timeline:

October 2003 Initial vendor notification.

November 2003 Notified vendor again via support IRC channels, verified reception of BugScan report.

January 2004 Vendor promised fix in upcoming 3.0 release.

December 2004 Trillian 3.0 released, second BugScan showed a few unfixed vulnerabilities remained.

February 2005 Contacted Trillian again, specifying locations of unfixed problems.

February 18, 2005 Contacted specific employees and forwarded the VSR. Received no response.

February 23, 2005 Contacted specific employees and forwarded the VSR. Received no response.

February 24, 2005 Trillian 3.1 update released with no additional security fixes from Trillian 3.0.

Securiteam: [NT] Trillian Plug-ins Buffer Overflow

ADDITIONAL INFORMATION

The information has been provided by
<mailto:matt.hargett@logiclibrary.com> Matt Hargett .

=====

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
In order to subscribe to the mailing list, simply forward this email to: 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.