

[NT] Trillian Pro Rendezvous XMPP HTML Decoding Heap Corruption

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-05/msg00009.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 7 May 2007 12:47:55 +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 Pro Rendezvous XMPP HTML Decoding Heap Corruption

SUMMARY

A vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Cerulean Studios Trillian Pro. Authentication is not required to exploit this vulnerability.

DETAILS

Vulnerable Systems:

- * Trillian Pro version 3.1 build 121

The specific flaw exists in the Rendezvous / XMPP (Extensible Messaging and Presence Protocol) messaging subsystem. Trillian locates nearby users through the '_presence' mDNS (multicast DNS) service on UDP port 5353. Once a user is registered through mDNS, messaging is accomplished via XMPP over TCP port 5298. Within plugins\rendezvous.dll the follow logic is applied to received messages:

```
4900C470 str_len:  
4900C470 mov cl, [eax] ; *eax = message+1  
4900C472 inc eax
```

[NT] Trillian Pro Rendezvous XMPP HTML Decoding Heap Corruption

```
4900C473 test cl, cl
4900C475 jnz short str_len

4900C477 sub eax, edx
4900C479 add eax, 128 ; strlen(message+1) + 128
4900C47E push eax
4900C47F call _malloc
```

The string length of the the supplied message is calculated and a heap buffer in the amount of length + 128 is allocated to store a copy of the message which is then passed through `expatxml.xmlComposeString()`, a function called with the following prototype:

```
plugin_send(MYGUID, "xmlComposeString", struct xml_string_t *);
```

```
struct xml_string_t {
unsigned int struct_size;
char *string_buffer;
struct xml_tree_t *xml_tree;
};
```

The `xmlComposeString()` routine calls through to `expatxml.19002420()` which, among other things, HTML encodes the characters `&`, `>` and `<` as `&`, `>` and `<` respectively. This behavior can be seen in the following disassembly snippet:

```
19002492 push 0
19002494 push 0
19002496 push offset str_Amp ; "&"
1900249B push offset ampersand ; "&"
190024A0 push eax
190024A1 call sub_190023A0

190024A6 push 0
190024A8 push 0
190024AA push offset str_Lt ; "<"
190024AF push offset less_than ; "<"
190024B4 push eax
190024B5 call sub_190023A0

190024BA push
190024BC push
190024BE push offset str_Gt ; ">"
190024C3 push offset greater_than ; ">"
190024C8 push eax
190024C9 call sub_190023A0
```

As the originally calculated string length does not account for this string expansion, the following subsequent in-line memory copy operation within `rendezvous.dll` can trigger an exploitable memory corruption:

[NT] Trillian Pro Rendezvous XMPP HTML Decoding Heap Corruption

```
4900C4EC mov ecx, eax
4900C4EE shr ecx, 2
4900C4F1 rep movsd
4900C4F3 mov ecx, eax
4900C4F5 and ecx, 3
4900C4F8 rep movsb
```

Note that binary data can be transmitted across the XMPP protocol via UTF-8 encoding.

Vendor Response:

Cerulean Studios has issued an update to correct this vulnerability. More details can be found at: <http://blog.ceruleanstudios.com/>

Disclosure Timeline:

2007.02.15 – Vulnerability reported to vendor
2007.05.02 – Digital Vaccine released to TippingPoint customers
2007.05.02 – Coordinated public release of advisory

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2418>
CVE-2007-2418

ADDITIONAL INFORMATION

The information has been provided by [mailto:Pedram Amini, TippingPoint Security Research Team](mailto:Pedram.Amini@TippingPoint.com) Pedram Amini, TippingPoint Security Research Team.

The original article can be found at:

<http://dvlabs.tippingpoint.com/advisory/TPTI-07-06>
<http://dvlabs.tippingpoint.com/advisory/TPTI-07-06>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.