

xchat IRC session hijacking vulnerability (versions 1.4.1, 1.4.2)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-01/0107.html>

From: zen-parse (zen-parse@gmx.net)

Date: 01/09/02

Date: Wed, 9 Jan 2002 22:45:13 +1300 (NZDT)

From: zen-parse <zen-parse@gmx.net>

To: <bugtraq@securityfocus.com>

=====
===== xchat 1.4.2 and 1.4.3 IRC session hijacking vulnerability =====
=====

It is possible to trick xchat IRC clients (1.4.2, 1.4.3) into sending commands to the IRC server they are on, potentially allowing for social engineering attacks, channel takeovers, and denial of service.

Vendor updates for affected versions soon.

=====
===== Background =====
=====

The CTCP PING reply handler is designed to return the string that was sent to it by another client. This enables that client to determine the time lag between them and another user.

The querying client types

/ping nick

which sends a command of the form:

```
PRIVMSG nick :\x01PING 1027050764\x01\n
```

Where "1027050764" was some representation of the current time, and \x01 is the character with the ASCII value 0x01.

The queried client would respond with:

```
NOTICE nick :\xPING 1027050764\x01\n
```

and the querying client would then compare the current time with the time in the string.

If you sent "test 1 2 3 4" as the time part, xchat would reply with the same string.

SecurityFocus Bugtraq: xchat IRC session hijacking vulnerability (versions 1.4.1, 1.4.2)

The xchat client also has a feature which allows insertion of arbitrary ascii valued characters into a message.

The message "This is %065 test." gets sent as "This is A test." to the server. (This option is disabled by default in later versions.)

If these expressions are expanded on the sending client, a ping message could be sent to a user with the command:

```
/msg nick %001PING 12345678%001
```

which would send a string like:

```
PRIVMSG nick :\x01PING 12345678\x01
```

(To disable expansion in xchat when you are typing them, use '%nnn' to send the '%nnn' literal. Eg: to send '%100x', type '%%100x' in the client. If your client does expansion, it would show up as 'dx', which can be quite annoying when discussing format strings.)

```
=====
===== The Problem =====
=====
```

The PING reply handler also expands the %nnn values in replies in the vulnerable clients.

Example exploit, By Marcus Meissner <Marcus.Meissner@caldera.de>

#fupp is a channel.

Victim is on it and has channel op status.

Enter the command: cat xchat.exploit - | netcat server 6667

(The - is necessary so we do not quit instantly)

This causes vulnerable 'Victim' to give user 'exploit' channel operator status in channel '#fupp' on server 'server'.

-- zen-parse

```
=====
= ObSpam: http://mp3.com/cosv/ - You know I want you to. =
=====
= 1337sp34|< @ |r(://|r(.pu|theplug.(0m/ {#r00th@t,#s0c|a|} @n|) 5tuff. =
=====
```

- 1) If this message was posted to a public forum by zen-parse@gmx.net, it may be redistributed without modification.
- 2) In any other case the contents of this message is confidential and not to be distributed in any form without express permission from the author.

- TEXT/PLAIN attachment: [xchat.exploit](#)
-

- *Previous message:* [jG gM: "dtterm exploit in Unixware 7.1.1"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)