

[UNIX] XChat /dns Command Execution Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0117.html>

From: support@securiteam.com

Date: 03/28/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 28 Mar 2002 12:55:12 +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 /dns Command Execution Vulnerability

SUMMARY

<<http://www.xchat.org/>> XChat is an IRC client for UNIX operating systems. I.R.C. is Internet Relay Chat, see <<http://irchelp.org/>> <http://irchelp.org/> for more information about IRC in general. A security vulnerability in the product allows attackers to cause the program to execute arbitrary commands.

DETAILS

There is an issue by the way XChat handle the /exec command, and more accurately in the /dns command. The /dns should resolve the host of somebody, by issuing the command "/dns some_nick" and program actually executes it via string replacement ("%s %s"), where the first string replaced is the DNS program name (filename), and the second is the hostname of the person you want to resolve.

Looking into the code of the program, i.e. the cmd_dns() function, you will find the following around common/outbound.c line 1474

```
{  
    sprintf (tbuf, "/exec %s %s", prefs.dnsprogram, nick);  
    handle_command (tbuf, sess, 0, 0);
```

}

And far away, at line 1863 in the cmd_exec() function:
execl ("/bin/sh", "sh", "-c", cmd, 0);

No dangerous characters are stripped out of cmd, allowing an attacker to force a server to respond to DNS query with ";DISPLAY=localhost:0.0;xterm". This would cause the command passed to the execl function to be as follows: "host;DISPLAY=localhost:0.0;xterm", which as you probably guessed it will execute an arbitrary command.

To exploit the hole, the attacker would need to force a server to respond to a whois command with a malformed DNS response.

Migrating factors:

- * An attacker must run his own specially patched server.
- * An attacker has to cause the user to the /dns command on someone.

ADDITIONAL INFORMATION

The information has been provided by <mailto:spacewalker@altern.org>
SpaceWalker.

=====

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] d_path() Truncating Excessive Long Path Name Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)