

Vulnerability in multiple "now playing" scripts for various IRC clients

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-08/msg00161.html>

- *From:* Wouter Coekaerts <wouter@xxxxxxxxxxxxx>
 - *Date:* Sun, 12 Aug 2007 19:02:24 +0200
-

In October 2006 I discovered many "now playing" scripts for various IRC clients allow an attacker to send commands to the IRC server on behalf of the user.

Details

=====

Many scripts for various IRC clients, that report the name of the currently playing song in a media player on IRC share the same security bug. They don't sanitize the name of the song before sending it to the IRC server. When a user plays a song with a newline (LF or CR, which are both message separators in IRC) in the name of a song, and uses such a script, the text following the newline will be interpreted by the IRC server as another command. Exploitation requires the attacker to trick a user into playing such a specially crafted song, and to then use his script while the song is playing. That makes it hard, but not impossible to exploit in practice. It results in the ability to execute IRC commands in the client of the victim. This could be abused, for example, to gain operator privileges on chat channels.

Because it requires so much user interaction to exploit, and the results are limited to sending commands to IRC, I'd call this a minor problem.

Affected

=====

What makes this bug noteworthy in my opinion is that it is present in **all** scripts with this feature which were tested. They can all be exploited by the same malicious mp3. This includes:

* irssi: from <http://irssi.org/scripts/>: ixmmsa.pl 0.3, l33tmusic.pl 2.00, mpg123.pl 0.01, ogg123.pl 0.01, xmms.pl 2.0, xmms2.pl 1.1.3, xmmsinfo.pl 1.1.1.1

* XChat: many from <http://xchat.org>: xmms-thing 1.0, XMMS Remote Control Script 1.07, Disrok 1.0, a2x 0.0.1, Another xmms-info script 1.0, XChat-XMMS 0.8.1, and more...

* weechat: from <http://weechat.flashtux.org/>: now-playing.rb, xmms.pl 1.1

* BitchX: from <http://scripts.bitchx.org/>: xmms.bx 1.0

* Konversation: included media script

* Many scripts for mIRC, and probably other clients too

Related bug

Vulnerability in multiple "now playing" scripts for various IRC clients

=====

Similarly, but worse, some scripts/plugins made for mirc don't remove | characters, which is a command separator in mirc. This allows arbitrary command execution (on the client, not just to the server), without needing more user interaction than just starting to play the file. For example