

[Full-Disclosure] Re: Terminal Emulator Security Issues

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-02/0358.html>

From: Michael Jennings (mej@eterm.org)

Date: 02/25/03

From: Michael Jennings <mej@eterm.org>
To: H D Moore <termulation@digitaloffense.net>
Date: Tue, 25 Feb 2003 12:28:38 -0500

(vulnwatch -> vulndiscuss at the request of the moderator)

On Tuesday, 25 February 2003, at 08:07:08 (-0600),
H D Moore wrote:

> *Would stripping escape sequences from the window title work? Do you
> know of any applications that actually use this feature?*

Well, my gut reaction was a patch which removed all characters less than 32 from the title and icon name when setting them, and when fetching them for display changed all such characters to blanks. That would effectively disable any carriage returns/linefeeds, escape codes, shift-in/shift-out, etc. (Incidentally, I was unable to embed any such sequences in the title/icon name in 0.9.2 anyway...but I didn't try for very long, so I may have missed something.)

While that would certainly disable the ability for the commands to be hidden from the user the way you mentioned (which actually tends to be ineffective on Eterm anyway, since most people don't use solid colored backgrounds...but I digress :)), as your sample showed, it is still possible to throw a sequence of commands up onto the terminal, requiring only the press of an Enter key on the part of the user.

And as UNIX (esp. Linux) gains mainstream acceptance, more novices will be using it. Since the UNIX command line is indistinguishable from line noise by the typical novice, it's not a far leap to think that one of them might pay attention to the "Press Enter" part (likely the only part which would make sense to them), not realizing the affect the command might have. Especially if it didn't produce any output.

So I guess it boils down to a question of, where does "social engineering" end and "user ignorance/stupidity" begin? I think some

Full-Disclosure: [Full-Disclosure] Re: Terminal Emulator Security Issues

discussion on that topic would be beneficial, at least for developers like me who would always rather do a feature right than not do it at all.

And no, I'm not aware of any application which uses that feature, but with the recent batch of "shell prompt theming" applications (bashish, and the like), I wouldn't be at all surprised if there was one.

- > *Absolutely correct, this paper was written over a period of months,*
- > *the 0.9.1 release was the latest version available with most*
- > *distributions when I made that claim. The reasons for picking on*
- > *Eterm:*
- >
- > ** arbitrary command execution at one point in its lifetime*

Yup. Major brain fart there. It was always intended solely as an interim measure, but I failed to fully consider its implications.

- > ** arbitrary file creation with user-defined content (via clear screen)*
- > ** shared feature-sets with xterm, rxvt, etc*
- > ** great documentation for all of these features ;)*

If only users were as thorough in their perusal of the documentation as you were.... :-)

- > *The vendor coordination was done through the vendor-sec mailing list*
- > *with about a three-week head start prior to disclosure. There really*
- > *weren't many true "bugs" found, just about everything covered was*
- > *implemented deliberately and could be found in the documentation of*
- > *the app. There had already been a number of debates on the*
- > *exploitability of these features, so this paper was more of a FAQ*
- > *than any sort of advisory. It wasn't my intention to catch anyone*
- > *off-guard on this, just to bring these issues back into the*
- > *limelight for a while and see if other people had a similar take on*
- > *them.*

Understood. As I mentioned, the only thing you mentioned that I didn't know of (and the only thing to which 0.9.2 is vulnerable) was the title setting issue, which I would just like to say was an absolutely **brilliant** piece of work. Never would I have thought to combine such a seemingly innocuous feature with a creative bit of social engineering to such a potentially devastating effect.

Truly impressive, as was the report overall. Kudos. :)

Michael

--

Michael Jennings (a.k.a. KainX) <http://www.kainx.org/> <mej@kainx.org>
n + 1, Inc., <http://www.nplus1.net/> Author, Eterm (www.eterm.org)

Full-Disclosure: [Full-Disclosure] Re: Terminal Emulator Security Issues

"I don't care if you win or lose, just as long as you win."

-- Vince Lombardi

Full-Disclosure - We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>