Xterm code execution via font ops (openwall.com)

65 points by jwilk 15 days ago | hide | past | favorite | 40 comments

vngzs 15 days ago | next [–]

```
-- $XTermId: README,v 1.3 2007/05/24 19:49:19 tom Exp $
-- Below is the original README for xterm from 1991, for your amusement.
-- For a better overview, see http://invisible-island.net/xterm/

                    Abandon All Hope, Ye Who Enter Here


This is undoubtedly the most ugly program in the distribution.  It was one of
the first "serious" programs ported, and still has a lot of historical baggage.
Ideally, there would be a general tty widget and then vt102 and tek4014
subwidgets so that they could be used in other programs.  We are trying to
clean things up as we go, but there is still a lot of work to do.

If you are porting this to a machine that has problems with overlapping
bcopy's, watch out!

There are two documents on xterm: the man page, xterm.man, which describes
how to use it, and ctlseqs.ms, which describes the control sequences it
understands.
```

nonrandomstring 15 days ago | parent | next [–]

There are so many modern, compact, versatile Xterm compatible terminal emulators that can be aliased. Is there any serious reason in 2022 to still be distributing instead of dragging it out behind the woodshed with a shovel.

somat 15 days ago | root | parent | next [–]

There is a quote.

Around computers it is difficult to find the correct unit of time to measure progress. Some cathedrals took a century to complete. Can you imagine the grandeur and scope of a program that would take as long?

```
-- Epigrams in Programming, ACM SIGPLAN Sept. 1982
```

Well, we have our cathedrals in programing, only we as as software engineers tend to be barbarians and call them "legacy code" or "obsolete systems" or "needs to be torn down and replaced with something new". Think of when people do this to actual cathedrals.

I like xterm, use it daily, I think Thomas Dickey is a pretty great guy for his role in maintaining the program.

https://www.invisible-island.net/xterm/xterm.html

nonrandomstring 15 days ago | root | parent | next [–]

Now I feel deservably bad. Xterm is is also part of my daily go-tos.

But then I look through apt or yum and see *so many* fresh faced usurpers, many written in modern languages... and also hear the same laments that Xterm is "unmaintainable". I didn't think of it as someone's cathedral. I'll put the shovel down. ;)

guenthert 15 days ago | prev | next [–]

"This does mean to exploit this vulnerability the user needs to be using Zsh in vi line editing mode (usually via $EDITOR having "vi" in it). While somewhat obscure this is not a totally unknown configuration."

I think by now, both users have adjusted their settings.

iudqnolq 15 days ago | parent | next [–]

If this happens automatically if EDITOR contains the substring "vi" then I'd guess this effects a significant portion of the xterm user base.

I don't think it does, though. This is based only on my rough memory that I used to use nvim and zsh and didn't notice that.

dgl 15 days ago | root | parent | next [–]

[Original finder here; I wrote that, I checked.]

See the docs: https://github.com/zsh-users/zsh/blob/f8d93888a8efd6c8142e74...

Relevant code: https://github.com/zsh-users/zsh/blob/f8d93888a8efd6c8142e74...

anarcat 15 days ago | prev | next [–]

as mentioned in the fine article, it looks like many distros patched this out already, for some reason. Debian has that default flipped since Debian *squeeze*, published in 2011:

https://sources.debian.org/src/xterm/261-1/debian/changelog/...

so yeah, kind of a big deal, except not really, looks like some folks were already careful with that possibly dangerous setting. :)

classichasclass 15 days ago | prev | next [–]

Serious question: is xterm really entirely at fault here? Doesn't zsh get some of the blame?

> It so happens ^G is in Zsh when in vi line editing mode bound to "list-expand". Which can run commands as part of the expansion leading to command execution without pressing enter!

bawolff 15 days ago | parent | next [–]

I blame xterm.

Control sequences should not trigger key presses. That's a recipe for disaster.

I think its entirely reasonable for a terminal program to bind any key it wants to execute a command.

kazinator 15 days ago | parent | prev | next [–]

What if xterm the text "rm -rf .\n" in response to some character sequence; could we blame the shell, or rm?

skissane 15 days ago | parent | prev | next [–]

xterm is (arguably) implementing ECMA-48 wrong: replies to out-of-band strings (such as OSCs) should themselves be marked as out-of-band (by embedding them in an OSC/APC/DCS/PM, terminated with ST not BEL). Instead it is replying to an out-of-band command in-band.

However, I think the design of the Unix tty subsystem is also at fault here - out-of-band messages (OSC/APC/DCS/PM) should be filtered out by default and only delivered to processes which explicitly declare that they are expecting them.

That said, if zsh is putting the tty in raw mode, it is saying it wants everything the terminal will send it, so it needs to do that filtering itself.

ilyt 15 days ago | parent | prev | next [–]

Other example of "running stuff when you just use the shell without pressing enter" is say listing a git branches when you use completion so no.

The exploit is "sending something that looks like user input that can also contain ^G"

Beltalowda 15 days ago | parent | prev | next [–]

I don't see why; it just has a keybind for Control+G.

tyingq 15 days ago | prev | next [–]

Does make me wonder how many people are left that use xterm regularly. I still use it, solely because of muscle memory from when it was one of few options. But it seems like most unixy operating systems offer up something else as the default terminal. And xterm being xterm, it's a bit of work to get it running nicely with a decent font and cut/paste behavior. So you have to be pretty deliberate about wanting it.

badsectoracula 15 days ago | parent | next [–]

I use xterm as my only terminal since it has pretty much zero dependencies, opens instantly, it is very responsive, supports everything (it is kind of a defacto standard) and the UI is minimal (just a scrollbar).

jmclnx 15 days ago | root | parent | next [–]

I will do a me-too also.

I find xterm works great with tmux plus I can easily change font size on the fly without any issues. Change font sizes on other terminals is either not allowed or sometime (rarely) corrupts the display.

taviso 15 days ago | root | parent | prev | next [–]

I use it too, nothing is quite so configurable, feature rich or reliable. I'll admit that XtTranslations are not user friendly, but they are powerful!

p_l 15 days ago | root | parent | prev | next [–]

There's a menubar and context menu, but one needs to know how to enable them in the first place ;)

UI_at_80x24 15 days ago | parent | prev | next [–]

I use it for cross-site compatibility primarily. I connect to hundreds of various *nix servers. Various Linux, FreeBSD, OpenBSD, and AIX. I don't notice font differences much (I'm half blind, so everything is rather large on my screen (and all fonts are kinda fuzzy)).

But what I do notice is that xterm is the only program that shows things like ncurses (i.e. mc, tree, etc.), and tmux, and language/locale correctly on everything.

I can get 1-2 of the above items but never all of them. (Konsole does a great job too, but xterm opens faster on my i3 setup.) I've manipulated my various dotfiles, and tried multiple combinations but xterm works 100% of the time.

bitwize 15 days ago | root | parent | next [–]

Xterm is a little behind the curve in some areas. For example I'm not sure that it properly handles color emoji -- and many modern hipster dev tools of the sort likely to shit ANSI color codes to stdout without even bothering to check if stdout is a tty, are also prone to using emoji for things like checkmarks for passing tests. (Homebrew, in particular, uses U+1f37a, BEER MUG, to indicate it has completed operations.)

But maybe you don't care about that. 90% of the time, I don't.

UI_at_80x24 15 days ago | root | parent | next [–]

Luckily I haven't encountered that. I'm almost of the opinion that all my servers should have locale LANG set to C and avoid all the UTF-8 headaches.

I don't want my servers to be cutesy.

bitwize 15 days ago | parent | prev | next [–]

Xterm is very broadly compatible with VT220 terminals, with some VT320 and VT420 features thrown in. It is a *terminal* emulator.

Other TEs, especially libvte-based ones, are more like crappy xterm emulators.

So there are reasons to want xterm, specifically.

anthk 15 days ago | root | parent | next [–]

XTerm has a keyboard locking mode, so X11 tools can't snoop it.

Other terms as you say, suck.

BTW, does this work under OpenBSD and ksh with "set -o vi"?

dgl 15 days ago | root | parent | next [–]

This exact variant with no interaction code execution doesn't, but it's possible to use the vi line editing keys via this bug and do something like hide a command before the current cursor position. (OpenBSD's ksh will show a little "<" in that case.)

jstimpfle 15 days ago | parent | prev | next [–]

I still use it, even though I have to configure fonts meticulously, and switching from the default font is a pain (no ctrl+mousewheel trick, can only select between 5 preconfigured fonts).

It starts up fast and reads text comparably fast, and it works great with most console programs. It doesn't try to reflow text when resizing, which simply can't be done correctly. Most other terminals try to reflow and it is frequently a mess (last I checked is long ago)...

Another reason I like xterm is that it's one of the few left that support bitmap fonts, and on old low-res screens those are much better legible. (On more modern displays with DPI > 150, it starts to become difficult to find large enough bitmap fonts.)

bitwize 15 days ago | root | parent | next [–]

Say 'xterm -fa <your favorite terminal font here>'. Boom, done. You can even use Xft font format, like "Terminus:pixelsize=20" rather then the traditional -blah-terminus-*-20-et-weary-cetera.

You can also set .Xresources, but that's a bit more complicated.

jstimpfle 15 days ago | root | parent | next [–]

I need to switch fonts in the current terminal, not start a new one. So yes, I'm setting fonts in .Xresources. It might not make a huge lot of sense for vector fonts, because I believe you can configure only 1 (can't check now). But for bitmap fonts, you can configure like 5 and then switch between them in the current terminal using control+right click -> select font.

anthk 15 days ago | parent | prev | next [–]

XTerm has a keyboard input locking mode thru the menus, making secure inputting of passwords doable. Not even X11 tools can sniff it.

pmarin 15 days ago | parent | prev | next [–]

Xterm is the only one I have used in Unix since 1996.

jwilk 15 days ago | prev | next [–]

I tried to put "<375" in the submission title, but HN would truncate the title just before "<".

taviso 15 days ago | prev | next [–]

I think the mitigation advice is incomplete, allowFontOps is disabled by default, so the mitigation is only necessary if you've enabled it.. but in that case you would need to put 'allowFontOps: false' *after* the stanza enabling it, right?

jwilk 15 days ago | parent | next [–]

> allowFontOps is disabled by default

It's enabled by default upstream.

https://invisible-island.net/xterm/manpage/xterm.html#VT100-...

taviso 15 days ago | root | parent | next [–]

That's what the manual on fedora says too, but it is disabled by default. I admit, I didn't try building from pristine source, so it could be patched!

jwilk 15 days ago | root | parent | next [–]

It looks patched indeed:

https://src.fedoraproject.org/rpms/xterm/blob/rawhide/f/xter...

taviso 15 days ago | root | parent | next [–]

Ah-ha, I stand corrected :)

dgl 15 days ago | root | parent | next [–]

Debian's patch is nicer, as the build process pulls the default from the man page, so: https://sources.debian.org/patches/xterm/375-1/904_fontops.d...

jwilk 15 days ago | root | parent | next [–]

> the build process pulls the default from the man page

Interesting idea, but I don't think that's what happens:

https://sources.debian.org/src/xterm/375-1/debian/rules/#L22

midislack 15 days ago | prev [–]

zsh considered harmful, not for the first time. This is why I use pdksh.

somat 15 days ago | parent [–]

For those of us who like the openbsd ksh(all two of us) which is derived from pdksh. there is the project oksh.

https://github.com/ibara/oksh

I don't know if this is helpful or just annoying unsolicited "advice"