Date: Sun, 30 Jan 2022 12:27:38 -0500
From: nick black <dankamongmen@...il.com>
To: oss-security@...ts.openwall.com
Subject: xterm buffer overflow via crafted sixel

howdy! in the hopes of further distributing my computing into
your terminal emulators, i this morning learned that i can
control writes to memory from XTerm's context via the method of
crafted sixel. en garde, i'll let you try my wu-tang style.

this was discovered while working on Notcurses bug #2573:

 https://github.com/dankamongmen/notcurses/issues/2573

an error of mine own led to emission of a corrupted sixel [0], and
spectacular gyrations from XTerm:

```
==1426124== Invalid write of size 2
==1426124==    at 0x193FF1: set_sixel (graphics_sixel.c:181)
==1426124==    by 0x1949E1: parse_sixel (graphics_sixel.c:534)
==1426124==    by 0x17203D: do_dcs (misc.c:4973)
==1426124==    by 0x149E03: doparsing.constprop.0 (charproc.c:4224)
==1426124==    by 0x14B383: VTparse (charproc.c:5183)
==1426124==    by 0x14B670: VTRun (charproc.c:8163)
==1426124==    by 0x12DC49: main (main.c:2911)
==1426124==  Address 0xffffffff0941efb8 is not stack'd, malloc'd or (recently) free'd
==1426124==
==1426124==
==1426124== Process terminating with default action of signal 11 (SIGSEGV): dumping core
==1426124==  Access not within mapped region at address 0xFFFFFFFF0941EFB8
==1426124==    at 0x193FF1: set_sixel (graphics_sixel.c:181)
==1426124==    by 0x1949E1: parse_sixel (graphics_sixel.c:534)
==1426124==    by 0x17203D: do_dcs (misc.c:4973)
==1426124==    by 0x149E03: doparsing.constprop.0 (charproc.c:4224)
==1426124==    by 0x14B383: VTparse (charproc.c:5183)
==1426124==    by 0x14B670: VTRun (charproc.c:8163)
==1426124==    by 0x12DC49: main (main.c:2911)
```

I reported this to Mr. Thomas Dickey, the Archfather, and
offered to put a patch together this evening. I also told him I
probably wouldn't bother with a CVE, regarding which I clearly
changed my mind pretty much immediately. Sorry, my good man =\.

This requires that XTerm was built with Sixel support, and that
the XTerm configuration interprets Sixels.

--nick

[0] "a man of genius makes no mistakes -- his errors are
  volitional, and the portals to discovery." (james joyce).
  nah, just kidding, i totally screwed it up.

--
nick black -=- https://www.nick-black.com
to make an apple pie from scratch,
you need first invent a universe.

Download attachment "signature.asc**" of type "**application/pgp-signature**" (834 bytes)**

Confused about mailing lists and their use? Read about mailing lists on Wikipedia and check out these guidelines on proper formatting of your messages.