Date: Wed, 10 Feb 2021 01:12:21 +0530
From: Utkarsh Gupta <utkarsh@...ian.org>
To: oss-security@...ts.openwall.com
Subject: Re: screen crash processing combining characters

Hi,

On Tue, 9 Feb, 2021, 9:39 pm Tavis Ormandy, <taviso@...il.com> wrote:

> Hello, I noticed someone posted this to the screen-devel list. I can
> reproduce it here, just catting the testcase does crash my screen
> session.
>
> https://lists.gnu.org/archive/html/screen-devel/2021-02/msg00000.html
>
> (I think it wasn't supposed to be public, but it is, so better it's
> visible to security teams)
>
> It looks like it might be exploitable at first glance, I see a crash
> here in encoding.c, because i is out of range.
>
> 1411   else if (!combchars[i])
> 1412   {
> 1413   combchars[i] = (struct combchar *)malloc(sizeof(struct
> combchar));
> 1414   if (!combchars[i])
> 1415   return;
> 1416   combchars[i]->prev = i;
> 1417   combchars[i]->next = i;
> 1418   }
>
> Exploitable or not, it would be annoying if someone stuffed this into
> logfiles
> being tailed, or whatever.
>

Got CVE-2021-26937 assigned for this.

- u

>