

Follow @Openwall on Twitter for new release announcements and other news

[\[<prev\]](#) [\[next>\]](#) [\[thread-next>\]](#) [\[day\]](#) [\[month\]](#) [\[year\]](#) [\[list\]](#)

Date: Tue, 9 Feb 2021 16:06:07 -0000 (UTC)
From: Tavis Ormandy <tavis@...il.com>
To: oss-security@...ts.openwall.com
Subject: screen crash processing combining characters

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.

Tavis.

```
--
_o)      $ lynx lock.cmpxchg8b.com
7\ \ _o) _o) $ finger tavis@....org
_ \_v _() _() @tavis
```

Powered by [blists](#) - more mailing lists

Please check out the [Open Source Software Security Wiki](#), which is counterpart to this [mailing list](#).

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

