Date: Thu, 19 Nov 2020 19:51:04 +0100
From: Moritz Mühlenhoff <jmm@...til.org>
To: oss-security@...ts.openwall.com
Subject: Re: libass ass_outline.c signed integer overflow

On Thu, Nov 19, 2020 at 11:54:07AM -0500, David A. Wheeler wrote:
> >> In `ass_outline_construct`'s call to `outline_stroke` a signed integer
> >> overflow happens *(undefined behaviour)*. On my machine signed overflow
> >> happens to wrap around to a negative value, thus failing the assert.
> >> https://github.com/libass/libass/issues/431
> >>
> >> https://github.com/libass/libass/pull/432
> >
> > I have followed the links above, and this seems to be an example of a
> > situation where the CVE process has failed. It is still not fixed in
> > Debian, possibly for that reason. I'll report a Debian bug today.
>
> I read through the issue discussion. As best as I can tell, no one filed for a CVE, so there was no CVE.
> Did I misunderstand something?
>
> If my understanding is correct, that is *NOT* a failure of the CVE process.

Yes, everything worked as designed here. This is CVE-2020-26682

Cheers,
        Moritz