

[Products](#)[Services](#)[Publications](#)[Resources](#)[What's new](#)

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

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

Message-Id: <C01HSHA08E4Q.HY2J0SF11I0@sumire>  
Date: Wed, 02 Nov 2022 04:33:19 +0100  
From: "alice" <alice@...ya.dev>  
To: <oss-security@...ts.openwall.com>  
Subject: Re: OpenSSL X.509 Email Address 4-byte Buffer  
Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer  
Overflow (CVE-2022-3786)

On Wed Nov 2, 2022 at 3:53 AM CET, Alex Gaynor wrote:  
> Alpine Linux switched to LibreSSL for a while, but then switched back  
> to OpenSSL. (LibreSSL is still packaged separately)  
(and nothing is meant to use libressl- things wanting the libtls  
interface from libressl link to libretls[0] instead, in general. (just  
for context, in alpine))

[0]: <https://git.causal.agency/libretls/about/>

>  
> Alex  
>  
> On Tue, Nov 1, 2022 at 10:53 PM Demi Marie Obenour  
> <demi@...isiblethingslab.com> wrote:  
> >  
> > On Tue, Nov 01, 2022 at 09:52:59PM +0100, Erin Shepherd wrote:  
> > > LibreTLS does not track the OpenSSL API, so increasingly software does not build with it (it's not  
> > > possible to support both LibreSSL and a supported version of OpenSSL without #ifdef hell)  
> >  
> > Has software not from OpenBSD considered switching to LibreSSL outright?  
> > --  
> > Sincerely,  
> > Demi Marie Obenour (she/her/hers)  
> > Invisible Things Lab  
>  
>  
>  
> --  
> All that is necessary for evil to succeed is for good people to do nothing.

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](#).