

[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: <CAFRnB2U7V8PA997x+d_si+SN-_w0naoC9M6impMENR5jfHiGwA@mail.gmail.com>
Date: Tue, 1 Nov 2022 22:53:58 -0400
From: Alex Gaynor <alex.gaynor@...il.com>
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)

Alpine Linux switched to LibreSSL for a while, but then switched back to OpenSSL. (LibreSSL is still packaged separately)

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](#).