

[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: <1e5efc36-0cd4-45e2-b838-1493f9db6518@app.fastmail.com>
Date: Tue, 01 Nov 2022 21:52:59 +0100
From: "Erin Shepherd" <erin.shepherd@...eu>
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)

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)

Additionally, there have been breakages to LibreSSL's compatibility with OpenSSL 1.0.

As a general rule, distros don't want to package multiple OpenSSL forks because it just heavily multiplies the amount of security work necessary.

On Tue, 1 Nov 2022, at 20:56, Demi Marie Obenour wrote:

> On Wed, Nov 02, 2022 at 06:35:42AM +1100, Dave Horsfall wrote:

> > On Tue, 1 Nov 2022, Demi Marie Obenour wrote:

> >

> > [Massive trim]

> >

> > > 3. When will OpenSSL be replaced by something written in a safe
> > > language, or at least with a better-maintained fork? I know that
> > > distributions often cannot use LibreSSL (because FIPS, ugh) or
> > > BoringSSL (because of no stable API or ABI), but I wonder if e.g.
> > > libcurl should be linked to BoringSSL instead.

> >

> > We see this over at <https://boringssl.goglesource.com/boringssl/> :

> >

> > ``Although BoringSSL is an open source project, it is not intended
> > for general use, as OpenSSL is. We don't recommend that third parties
> > depend upon it. Doing so is likely to be frustrating because there
> > are no guarantees of API or ABI stability.''

> >

> > If even the manufacturer says that you shouldn't use it...

>

> My understanding was that libcurl gets updated whenever BoringSSL needs
> a change, and that libcurl's API does not depend on what TLS backend it
> uses. Applications would not be impacted, since they would only use the
> libcurl API and ABI.

>

> That said, this would require constantly updating to new versions of
> libcurl + BoringSSL, so it might not make sense in general. LibreSSL or
> rustls could well be a better choice.

> --

> Sincerely,

> Demi Marie Obenour (she/her/hers)

> Invisible Things Lab

>

>

> *Attachments:*

> * signature.asc

[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](#).