

[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: <Y2F6C/dZo5njPUfd@itl-email>  
Date: Tue, 1 Nov 2022 15:56:57 -0400  
From: Demi Marie Obenour <demi@...isiblethingslab.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)

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.googleusercontent.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

**Download attachment "[signature.asc](#)" of type "application/pgp-signature" (834 bytes)**

[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](#).