```
Message-ID: <alpine.BSF.2.21.9999.2211020631160.34372@aneurin.horsfall.org>
Date: Wed, 2 Nov 2022 06:35:42 +1100 (EST)
From: Dave Horsfall <dave@...sfall.org>
To: OSS Security <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 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.googlesource.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...

-- Dave
```