```
Message-ID: <Y2K1yOB7748iGI2P@wopr>
Date: Wed, 2 Nov 2022 11:24:08 -0700
From: Kurt H Maier <khm@...ops.net>
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 03:09:21PM +0100, Hanno Böck wrote:
> FWIW it only takes a basically trivial fuzz target on the affected
> function to find this bug with libfuzzer.

I'm not sure what the value is of all this Monday-morning
quarterbacking, from 'basically trivial' fuzzing to code-quality
comparisons of hypothetical Rust ports.  OpenSSL's development process
has a bad rap, and there are definitely some easy wins to be had.
Posting "if they'd only adopted my pet practice" to oss-sec isn't fixing
anything in the OpenSSL project.  Please consider directing fuzzing
advice and PL theory directly to the project?  I agree there would be
benefit to this stuff, but dunking on them on unrelated lists isn't
getting the medicine to the patient.

Respectfully,
khm
```