

[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: <Y2MAGbrZ07r23Wtp@gentoo.org>
Date: Wed, 2 Nov 2022 18:41:13 -0500
From: John Helmert III <ajak@...too.org>
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 11:24:08AM -0700, Kurt H Maier wrote:
> 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.

I don't read it (Hanno's point) as a 'dunk', some information on how
this kind of thing might be prevented in the future certainly has
value here.

>
> Respectfully,
> khm

Download attachment "[signature.asc](#)" of type "application/pgp-signature" (229 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](#).