Message-ID: <CAH8yC8mzcw-C257znYHH+qSyXoFVJWaAD=3dbvH3ZxymUtZU0A@mail.gmail.com>
Date: Tue, 1 Nov 2022 16:57:25 -0400
From: Jeffrey Walton <noloader@...il.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 Tue, Nov 1, 2022 at 3:55 PM Pavan Maddamsetti
<pavan.maddamsetti@...il.com> wrote:
>
> https://github.com/RustCrypto

I hope this does not start a war.. The problem with Rust is, it's only
guaranteed to work on i686 and x86_64.

Trying to compile Rust programs on armel, armhf, aarch64 and PowerPC
has been excruciatingly painful. The tool cannot compile its own
cargo's on those platforms. I gave up trying to use Rust on anything
but x86_64.

(Don't believe the marketing literature at
https://doc.rust-lang.org/beta/rustc/platform-support.html).

Jeff

> On Tue, Nov 1, 2022, 3:42 PM Dave Horsfall <dave@...sfall.org> 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.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...
> >