Message-ID: <20221102224300.xqyTm%steffen@sdaoden.eu>
Date: Wed, 02 Nov 2022 23:43:00 +0100
From: Steffen Nurpmeso <steffen@...oden.eu>
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)

Kurt H Maier wrote in
 <Y2K1yOB7748iGI2P@...r>:
 |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.

I never understood this way of seeing things.

Basically all the (non-military, at least) world was using it for
decades without giving back a kopek, and there were funny threads
on the ML, and basically that neat perl-based assembler production
system for even more speed-ups was a noticeable part of the
traffic.

So then heartbleed came and suddenly projects splitted off, but
luckily some funding was finally found for the OpenSSL project
itself, which made me cheer.

Since then more and more paid programmers are working there, and
have rewritten most of the code (i did not look as it is such
a detangled thing, like GNU C lib was twenty years ago, and until
you have found what you look for you have gray hair), added
myriads of tests, etc etc.

They also went to a public hoster and have thousands of issues as
more people look in the code as ever before (i would think, but
i was not looking at the community before ~2011).

I saw some odd naming issues, left-behind interfaces (that i like
a lot, mostly SSL_CONF_cmd() and <-> configuration files, but
unfortunately the road to sanity that this would allow was never
forcefully advertised; and this was somewhere before the 3.x
series was released, it could have been healed in the meantime).

It is not me alone that thinks that documentation misses
a straight path, i mostly live on "network security with OpenSSL"
that is a bit aged, so to say.
I personally have problems with the attitude too, the silent
openssl-dev@ i was on for a decade was replaced with a super
chatty thing that i left very quickly, i really hate their
announcements which link to some web site which basically says
a non-interactive sentence if you are lucky, so i always say
"thanks" and look upwards to the Olymp, basically.
Anyhow: my personal problem.

In short: where _so_ much work is done, and so many people work,
errors can surely happen.
I want to point out that other libraries which forked away often
simply copy code over from OpenSSL after that has done the work.
Not always, but it happens frequently.
I do not depreciate the fact, but it is one.

```
It is just that _i_ do not rub my very big balls (this does not
mean you, Kurt Maier) and point my finger at a project which is
the foundation for a very large part of _free_ and _open_ security
for the internet.

Donate for testing, maybe?  Dedicate time to write boring tests
maybe?  All you need to do is to become a member of that big thing
that does not like Iran, North Korea, Cuba, and i am a bit
misguided of who are the bad guys (evil states) at the moment,
it does not truly reflect my personal truth.  But so it is.

 |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.

Ah yes!
The number of tests is in fact driving me _insane_.  I track git..

--steffen
|
|Der Kragenbaer,                The moon bear,
|der holt sich munter           he cheerfully and one by one
|einen nach dem anderen runter  wa.ks himself off
|(By Robert Gernhardt)
```