Message-Id: <FFA5687C-C618-4896-A2C0-5CE992FEF632@gentoo.org>
Date: Thu, 3 Nov 2022 20:23:32 +0000
From: Sam James <sam@...too.org>
To: oss-security@...ts.openwall.com
Cc: nic.tuv@...il.com,
 Hanno Böck <hanno@...too.org>
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 3 Nov 2022, at 16:32, Nicola Tuveri <nic.tuv@...il.com> wrote:
>
> I can also add that at least this member of the OpenSSL Technical
> Committee is following the discussion, and I believe I am not the only
> one.
>
> The feedback shared here on oss-security is read and carefully
> considered, and I know it will be discussed within OTC to continue the
> ongoing process of improving the OpenSSL project and its procedures.

I'd like to thank the OpenSSL developers for being open to the
CI improvements I've been making lately.

>
> I totally concur with Tavis Ormandy:
>> this is active prolific opensource security researchers discussing their opensource security work on the
opensource security mailing list :)
>
> Personally, I'd like to thank you all for the feedback so far, as it
> is in itself a contribution to the project, even when it is harsh and
> reminds us of our mistakes.
> As long as it is kept polite and constructive, as it has been so far
> here, all feedback is very welcome and valuable.

Something I think that should be revisited is the priority
of undefined behaviour in the codebase.

Undefined behaviour can - and has [0][1] - led to misbehaviour
at runtime.

Part of living with "Modern C" is embracing the
techniques we have available to enhance compiler diagnostics
and detect problems. That includes LTO, as well, which
generally leads to _far_ better compiler warnings.

The OpenSSL codebase isn't strict aliasing clean, and in
Gentoo, we've built with -fno-strict-aliasing since ~2005
(note that -fstrict-aliasing is enabled by default with -O2
in GCC since at least 10 years ago).

If at all possible, I'd ask that the OpenSSL team revisit
its assessment of the severity of strict aliasing bugs
as well as the value of LTO in enhancing diagnostics
and finding bugs.

And if it's deemed to not be a priority at this time,
the build should enforce disabling them both.

Again, this isn't about performance - it's about:
1. Distributions inadvertently enabling something
which is unsafe/insufficiently tested (LTO), or
2. Not realising an option enabled by default
in standard configurations can lead to miscompiled

```
OpenSSL.

(For my part, I've been trying to improve CI but I've
also got some patches for aliasing bits which I'm
playing with.)

[0] https://github.com/llvm/llvm-project/issues/55255
[1] https://github.com/openssl/openssl/issues/18225
[2] https://github.com/openssl/openssl/issues/18663#issuecomment-1181478057

Best,
sam
```

Download attachment "signature.asc" **of type** "application/pgp-signature" **(359 bytes)**