

[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: <tk0n6j\$10pr\$1@ciao.gmane.io>
Date: Thu, 3 Nov 2022 15:36:51 -0000 (UTC)
From: Tavis Ormandy <taviso@...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 2022-11-02, 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.

Hanno and I have contributed months of programmer time on openssl research and produced a ton of CRITICAL/HIGH issues over the years, not to mention nss, gnutls, etc. What you're looking at isn't Monday-morning quarterbacking on an unrelated list - this is active prolific opensource security researchers discussing their opensource security work on the opensource security mailing list :)

Tavis.

```
--  
_o)          $ lynx lock.cmpxchg8b.com  
^\\ _o) _o) $ finger taviso@...org  
_\\_V _(`) _(`) @taviso
```

[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](#).