

[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: <tju633\$t4h\$1@ciao.gmane.io>  
Date: Wed, 2 Nov 2022 16:32:36 -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, Alex Gaynor wrote:

> In Rust, assuming you wrote normal safe Rust[0], and you had code that  
> overran a buffer on the stack, you'd get a panic() -- which is roughly  
> an abort (there's even a mode where it literally is an abort. By  
> default it unwinds and runs destructors and such). As a general rule,  
> bounds check issues aren't caught at compile time (in contrast with  
> temporal safety, which mostly is enforced at compile time.)  
>

Got it - thanks! It seems like in the specific case of non-exploitable overflows, rust wouldn't have made too much difference (abort() vs panic())... although obviously that doesn't mean other issues wouldn't have been mitigated.

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](#).