

[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: <tjtkiu\$jeu\$1@ciao.gmane.io>  
Date: Wed, 2 Nov 2022 11:33:50 -0000 (UTC)  
From: Tavis Ormandy <tavis@...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 2022-11-01, Jeffrey Walton wrote:  
> On Tue, Nov 1, 2022 at 3:55 PM Pavan Maddamsetti  
><pavan.maddamsetti@...il.com> wrote:  
>>  
>> <https://github.com/RustCrypto>  
>

I don't know rust, so serious question - if this same buggy punycode routine had been written in rust, what would have happened?

- I assume you *could* write similar logic, but perhaps the argument is that idiomatic rust discourages it?
- Would rustc have been able to reason about the code well enough at compile time to error out?
- Just detect it at runtime and abort()?

If the answer is "error out", then I think that's a pretty convincing win.

Tavis.

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

[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](#).