

[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: <20221102124527.05WVR%steffen@sdaoden.eu>  
Date: Wed, 02 Nov 2022 13:45:27 +0100  
From: Steffen Nurpmeso <steffen@...oden.eu>  
To: oss-security@...ts.openwall.com  
Subject: Re: 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 Wed, Nov 2, 2022 at 7:57 AM Tavis Ormandy <tavis@...il.com> wrote:  
|> I don't know rust, so serious question - if this same buggy punycode

The problem with punycode is punycode as such.  
It should have been URL-encoded UTF-8 maybe with normal decomposition from the start, and the DNS limits should have been raised, all that now well over twenty years ago.

Poul-Hennig Kamp of FreeBSD, varnish etc wrote just this week on another ML

|> The other thing to keep in mind is the immense existing codebase of  
|> unix kernels et al, not to mention application code depending on  
|> those kernels.

|This is the mistake we IT-people keep doing again and again:

|Forwards compatibility is /far/ more important than backwards compatibil\|  
|ity.

It would have been grown out by now. And many problems would never happened, including those incompatibilities that they wanted to avoid. My one cent.

Other than that. Sigh. C is the culprit!!

--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)

[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](#).