Ruby master - Bug #6233

Definition of EVP_MD_CTX_cleanup incomplete.

03/31/2012 07:57 AM - rubysubmit (Ruby Submit)

Status:	Closed	
Priority:	Normal	
Assignee:	openssl	
Target version:		
ruby -v:	ruby 1.9.2p290	**Backport:**

Description

File: ext\openssl\openssl_missing.c
Line: 67

```
#if !defined(HAVE_EVP_MD_CTX_CLEANUP)
int
EVP_MD_CTX_cleanup(EVP_MD_CTX ctx)
{
/ FIXME!!! */
memset(ctx, 0, sizeof(EVP_MD_CTX));

return 1;

}
#endif
```

History

#1 - 03/31/2012 08:27 AM - mame (Yusuke Endoh)

- Status changed from Open to Assigned

- Assignee set to MartinBosslet (Martin Bosslet)

Hello, emboss

What do you think?

--
Yusuke Endoh mame@tsg.ne.jp

#2 - 03/31/2012 09:19 AM - MartinBosslet (Martin Bosslet)

mame (Yusuke Endoh) wrote:

> Hello, emboss
>
> What do you think?

Hi, I think it's a valid point - here is how OpenSSL 1.0.1 implements it:

```
/* This call frees resources associated with the context /
int EVP_MD_CTX_cleanup(EVP_MD_CTX *ctx)
{
#ifndef OPENSSL_FIPS
/ Don't assume ctx->md_data was cleaned in EVP_Digest_Final,
* because sometimes only copies of the context are ever finalised.
/
if (ctx->digest && ctx->digest->cleanup
&& !EVP_MD_CTX_test_flags(ctx,EVP_MD_CTX_FLAG_CLEANED))
ctx->digest->cleanup(ctx);
if (ctx->digest && ctx->digest->ctx_size && ctx->md_data
&& !EVP_MD_CTX_test_flags(ctx, EVP_MD_CTX_FLAG_REUSE))
{
OPENSSL_cleanse(ctx->md_data,ctx->digest->ctx_size);
OPENSSL_free(ctx->md_data);
}
```

#endif
if (ctx->pctx)
EVP_PKEY_CTX_free(ctx->pctx);
#ifndef OPENSSL_NO_ENGINE
if(ctx->engine)
/The EVP_MD we used belongs to an ENGINE, release the
* functional reference we held for this reason. */
ENGINE_finish(ctx->engine);
#endif
#ifdef OPENSSL_FIPS
FIPS_md_ctx_cleanup(ctx);
#endif
memset(ctx,'\0',sizeof *ctx);

```
return 1;
}
```

Quite some additional cleansing besides the memset. We could simply copy this, but I'm afraid it could cause compatibility problems with older versions and we would additionally have to keep this in sync with what OpenSSL does there - both unpleasant situations. EVP_MD_CTX_cleanup was introduced in 0.9.7, I just checked. We claim compatibility from 0.9.6 on. I think the question must be allowed: do we really need compatibility with 0.9.6? It was released in 2000, 0.9.7 came in 2002. 10 years of backward compatibility aren't that bad either :) No but honestly, when I think of all the security fixes that came since then, nobody should really be running on 0.9.6 anymore anyway. I'm not against fixing this with the above and keeping the code in sync, but I'd be more happy with not having to poke around in implementation details and dropping 0.9.6 support instead.

But I'm not sure how this plays with the general principles of 2.0.0 or if anyone would be really against dropping 0.9.6 support. Opinions?

#3 - 03/31/2012 10:12 AM - mame (Yusuke Endoh)

Thank you for your quick reply.

Ultimately, everything about standard library is determined by
each maintainer. So, in general, you can go ahead if you think
it is appropriate.

I have no opinion about with this paticular case.
Is 0.9.6 still (effectively) maintained by OpenSSL team?
NaHi, do you have an opinion?

--
Yusuke Endoh mame@tsg.ne.jp

#4 - 03/31/2012 11:09 AM - MartinBosslet (Martin Bosslet)

mame (Yusuke Endoh) wrote:

> I have no opinion about with this paticular case.
> Is 0.9.6 still (effectively) maintained by OpenSSL team?

It says nothing about end of life on their home page, but
judging from the strategy of how they released security
fixes in the past it seems like only the last major release
will receive updates. For example while 0.9.8 was the version
in development, they also published maintenance releases
for 0.9.7, when 1.0.0 became the current series, they only
released additional versions of 0.9.8.

But that's just speculating, so I guess it's best if I ask
on their mailing list. Or maybe nahi knows more?

#5 - 09/13/2015 03:18 AM - zzak (Zachary Scott)

- Assignee changed from MartinBosslet (Martin Bosslet) to openssl

#6 - 05/28/2016 05:04 AM - rhenium (Kazuki Yamaguchi)

- Status changed from Assigned to Closed

r55162 (openssl: drop OpenSSL 0.9.6/0.9.7 support, 2016-05-25) removed the code.