PDF Export for report 3246519

Default Minimum TLS Version Set to TLS v1.0 (Cryptographic Weakness)

State	N/A
Reported by	MONKEY Dee (monkey_dee)
Reported to	curl (curl)
Submitted at	(ISO-8601)
Asset	
References	
Weakness	Use of a Broken or Risky Cryptographic Algorithm
Severity	Medium (4.0 ~ 6.9)
CVE IDs	

Activity

2025-07-10 21:42 manually disclosed Public

I understand. Well thanks for reviewing my report and considering the issue. I’m happy you took the time to look into it and move the discussion to the public mailing list. Thanks again for your response.

2025-07-10 21:35 comment Public

Per project policy for transparency, we want all reports disclosed and made public.

2025-07-10 21:25 agreed on going public Public

I just posted this:https://curl.se/mail/lib-2025-07/0007.html

2025-07-10 21:25 bug not applicable Public

Hey, thanks for getting back to me so fast. I get that old OpenSSL versions come with tons of risks, but I still think curl setting TLS v1.0 as the default minimum with CURL_SSLVERSION_DEFAULT can trip up users into using insecure setups, especially in places stuck with older libraries. How about bumping the default minimum to TLS v1.2 in curl’s code to keep users safer out of the box? I’m totally up for chatting more about this!

2025-07-10 21:09 comment Public

This is all documented behavior; not a vulnerability. Also, using an outdated TLS library version that was end-of-lifed already years ago most certainly brings a whole busload of more serious problems than this.

We could certainly discuss removing the possibility to set and use TLSv1.0, but that should be done in the open for all to participate.

2025-07-10 19:33 comment Public

Personally I do not see this as a security issue with curl eg. anyone building curl with a decade old version of openssl should not be surprised it might have serious security problems.

Of course I am ignoring the utility of backports and that some users have no choice ... but TLSv1 having issues with BEAST/POODLE ... it also has no good crypto algs ... and most browsers/os and 'stuff' have it disabled. Sometimes it is not possible to keep backporting things.

I will let others comment if we should do ban TLSv1 in curl. I am sure some users would complain.

2025-07-10 18:56 comment Public

Initial impression is one probably has more problems when using an older openssl ... and yes in the year 2025, one should never use TLS 1.0.

I guess the question then is should curl protect the user from doing this to themselves ... or maybe we can highlight in docs 'dont do this'.

2025-07-10 18:44 comment Public

Thank you for your report!

We will take some time and investigate your reports and get back to you with details and possible follow-up questions as soon as we can! Most likely within the next 24 hours.

We always strive to fix reported problems as fast as possible. Issues with severity Low or Medium we merge into the next release in the ordinary release cycle. Only for more serious problems we might release fix early.

2025-07-10 18:26 comment Public