
Subject: SSL protocol version

Posted by [Zbych](#) on Sun, 06 Oct 2013 20:30:44 GMT

[View Forum Message](#) <> [Reply to Message](#)

Hi,

When SSL context is created SSLv3_client_method is used. This restricts protocol version to v3. Can we change it to SSLv23_client_method, so v2, v3 and TLSv1 will be enabled? Or at least give user a choice?

```
bool TcpSocket::SSLImp::Start()
{
    LLOG("SSL Start");
    ...
    ERR_clear_error();
    if(!context.Create(const_cast<SSL_METHOD *>(SSLv23_client_method())) {
        SetSSLError("Start: SSL context.");
        return false;
    }
}
```

Subject: Re: SSL protocol version

Posted by [mirek](#) on Thu, 24 Oct 2013 17:36:44 GMT

[View Forum Message](#) <> [Reply to Message](#)

Zbych wrote on Sun, 06 October 2013 16:30Hi,

When SSL context is created SSLv3_client_method is used. This restricts protocol version to v3. Can we change it to SSLv23_client_method, so v2, v3 and TLSv1 will be enabled? Or at least give user a choice?

```
bool TcpSocket::SSLImp::Start()
{
    LLOG("SSL Start");
    ...
    ERR_clear_error();
    if(!context.Create(const_cast<SSL_METHOD *>(SSLv23_client_method())) {
        SetSSLError("Start: SSL context.");
        return false;
    }
}
```

OK, I can add an option. Would you care to provide a patch? (If not, I can do it anyway, but it will

take longer

Mirek
