interweb

Generated on 15/11/2026 00:10

KNOWLEDGE BASE · PUBLIC DOCUMENT

ERR_CONNECTION_CLOSED and ERR_SSL_VERSION_OR_CIPHER_MI when the error is not the server's

Site Down & Connection Errors

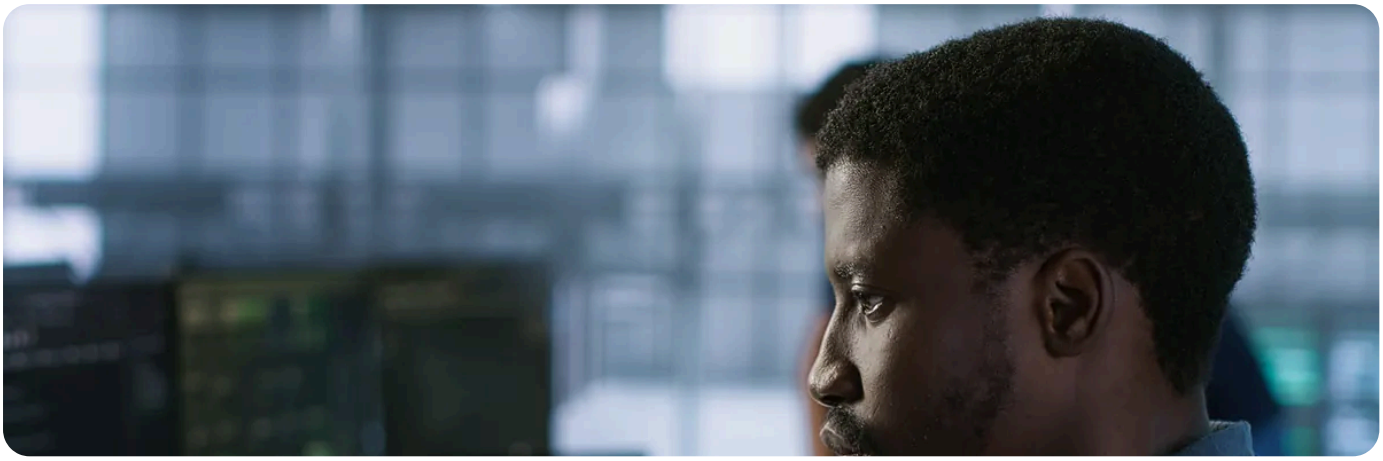
CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-714	v2026.10.18	Angola · English

Interweb Angola
RLX Angola, Lda. · Group RLX Holdings
Tax ID (NIF) 500 260 5724 · Commercial registration no. 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/714

ERR_CONNECTION_CLOSED and ERR_SSL_VERSION_OR_CIPHER_MISMATCH: when the error is not the server's

Site Down & Connection Errors · Created on **September 27, 2026** · Updated on **October 18, 2026** · 4 min read



Neither of these is an HTTP code. They are **messages from the browser itself**, and that changes everything: a 500 was produced by a server that answered; these were produced by your browser **because nothing answered at all**, or because what came back was not usable.

Which is why this article exists. "My site is down" and "this computer cannot reach it" look identical on screen, and they almost never are.

The thirty-second test that settles half the cases

1. Open the same address **on your phone with Wi-Fi turned off**, over mobile data. It is the most different network you have to hand.
2. If it opens on the phone and not on the computer, the site **is up**. The problem is the network, the computer or the browser you were on.
3. If it opens nowhere, then it is a different matter: follow **your site is down**.
4. Ask someone in another city or on another provider to try. Two different networks agreeing tells you far more than ten attempts on the same one.

ERR_CONNECTION_CLOSED: the connection opened and shut

The browser did reach something, and that something hung up halfway without saying why. Since there was no HTTP response, there is no number to read. The causes, most common first:

Cause	How to confirm it
Your IP address got blocked	The sign is unmistakable: it opens on mobile data and not at the office. See **why your IP gets blocked** and **how to unblock it**.
An antivirus or an extension inspecting traffic	Turn the extension off, or the antivirus feature that scans secure connections, and try again. Many of them sit in the middle of the connection, and some break it.
The network you are on	Company, school and some provider networks filter. If mobile data opens it and Wi-Fi does not, it is the network.
A VPN or a proxy	Turn it off and repeat. If it only fails with the VPN on, it is that path that is broken.
The name points somewhere else	If the domain points at an address where nothing lives any more, nobody picks up. Confirm with **how to check a domain DNS**.

ERR_SSL_VERSION_OR_CIPHER_MISMATCH: they did not agree

Here there was a conversation, and no agreement. To open a secure connection, browser and server must agree on a protocol version and on a set of ciphers. If one list does not overlap the other, the connection is never born, and the browser says exactly this.

Cause	What gives it away
The computer or the browser is old	This is cause number one. A system that no longer gets updates stops knowing the modern versions of the protocol. Sign: it fails on one computer and opens on every other one, phone included.
The computer's date and time are wrong	A certificate has a start and an end. With the clock off, everything looks invalid. Set the time automatically and retry.
A middleman on the wrong SSL mode	With Cloudflare in front, the SSL mode is the setting that has broken the most sites. See **switching on SSL at Cloudflare**.
The certificate does not cover that name	Happens with a brand-new subdomain, before its certificate is issued. See **no padlock on your site**.
An antivirus replacing the certificate	Some install a certificate of their own so they can read the traffic. When that goes wrong, this is the symptom.

Be careful with the "just ignore the warning" advice.
These errors exist to protect you. If they show up on a public network and only on that network, the possibility of someone sitting in the middle is real. Change network instead of working around the warning.

How to prove it without trusting the browser

Two command lines, the same on any system, tell you whether the server is answering and on what terms. Run them from the network where the site will not open, then from another one:

1. `curl -I https://yourdomain` returns the response headers. If anything comes back, the server answered and the problem is the browser or the path.
2. `openssl s_client -connect yourdomain:443` shows the secure handshake raw, including the protocol version agreed and the certificate served. If it fails here and works on another network, it is the network.
3. Compare against any other address you know is up. If everything fails from that network, the problem is not your site.

If you write to us, send both outputs as text

and say which network and what time. Add your public IP address, obtained as explained in **how to find your public IP address**: that is what lets us confirm whether it was our firewall.

NEED A HAND?

Opens on the phone but not on the computer? Send us your IP and the time.

Open a support ticket →

SEE ALSO

- SSL certificates →
- Support Policy →
- Frequently asked questions →

interweb

Interweb Angola

RLX Angola, Lda. · Group RLX Holdings

TAX ID (NIF)	500 260 5724
COMMERCIAL REGISTRATION NO.	26464-25/250724
REGISTERED OFFICE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACT	info@interweb.ao · +244 942 011 191 · www.interweb.ao
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

RLX-AO-KB-714 · v2026.10.18 · Generated on 15/11/2026 00:10

Online version of this document