Let's Encrypt expires root certificate, many devices and websites have problems accessing it

On September 30, 2021, Let's Encrypt's DST Root CA X3 root certificate expired and had to be replaced with a new one.

Let's Encrypt is one of the largest HTTPS certificate authorities in the world. Operating on a non-profit basis, Let's Encrypt issues certificates that encrypt the connection between your devices and the internet to ensure that no one can intercept and steal your data as it travels back and forth.

On September 30, 2021, Let's Encrypt's DST Root CA X3 root certificate expired and had to be replaced with a new one. The newly applied certificate is ISRG Root X1. This has caused access issues for a wide range of devices and websites globally. Free SSL sites, legacy devices, and iOS devices are most affected.

As announced by the company that owns the Let's Encrypt service, in most cases your system will automatically switch to the new certificate-based authentication chain. However, sometimes the expiration of the root certificate causes the certificates to be deemed untrusted or invalid.

To fix it, you need to make sure that the server (for admin) and device (for users) use the correct authentication string.

For sites that use free SSL, the admin can consider a new SSL alternative. After replacing the new SSL, the clients have to restart to be able to access the site.

Good luck with your fix!

tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.