Framework to test Preparedness against Quantum Computing

Authors:
Atish Joottun
Poshan Peeroo
Kevin Yerkiah

Co-Author:
Mr Anwar Chutoo

Affiliation:
University of Mauritius / Cyberstorm

Executive Summary

- **This Research analyses websites TLS servers**
- **This project can be scaled to other countries as well**
- **Rigorous validation of IP was done**
- **All the code is Open-Sourced and available on GitHub**

GitHub Link: https://github.com/AtishJoottun/Tldr_fail_testing

The TLDR Bug?

What is it?

- (TL;DR: Too Long; Didn’t Read).
- documented by David Benjamin in tldr.fail
- Reject connection made by large TLS ClientHello
- Does not negotiate for Classical Cryptography
- Closes the connection completely

Why does this happen?

- Misconfigured TLS servers
- Middle Box or Firewall flagged the packets
- A flawed TLS server can not read the multiple packets of Client Hello

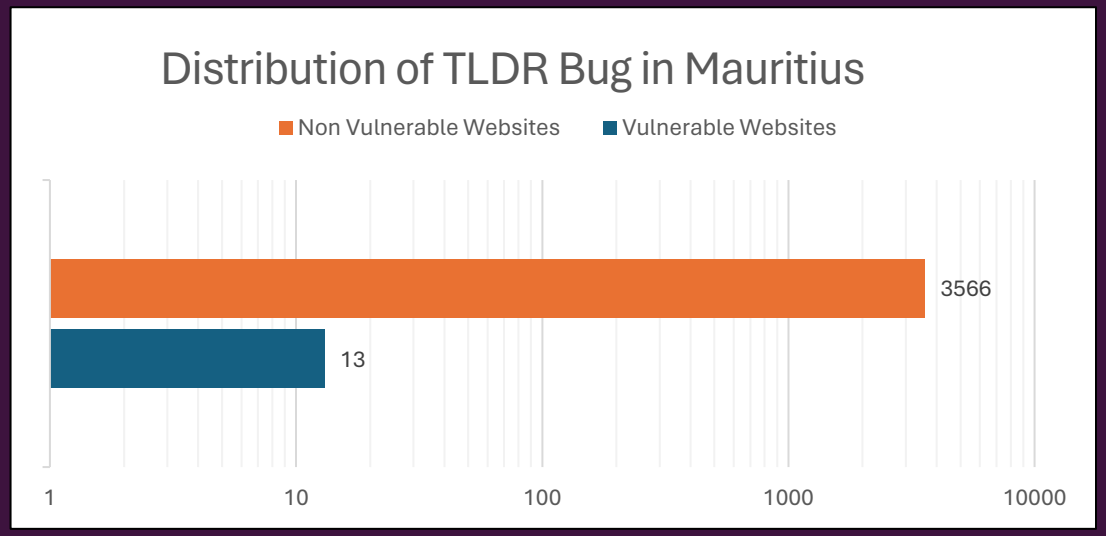
The testing of the IPs

Our process to analyze the websites are:

- **IP Addresses Collection**
- **Scalable Data Processing**
- **IP Validations**
- **Testing The IP for the TLDR Bug**

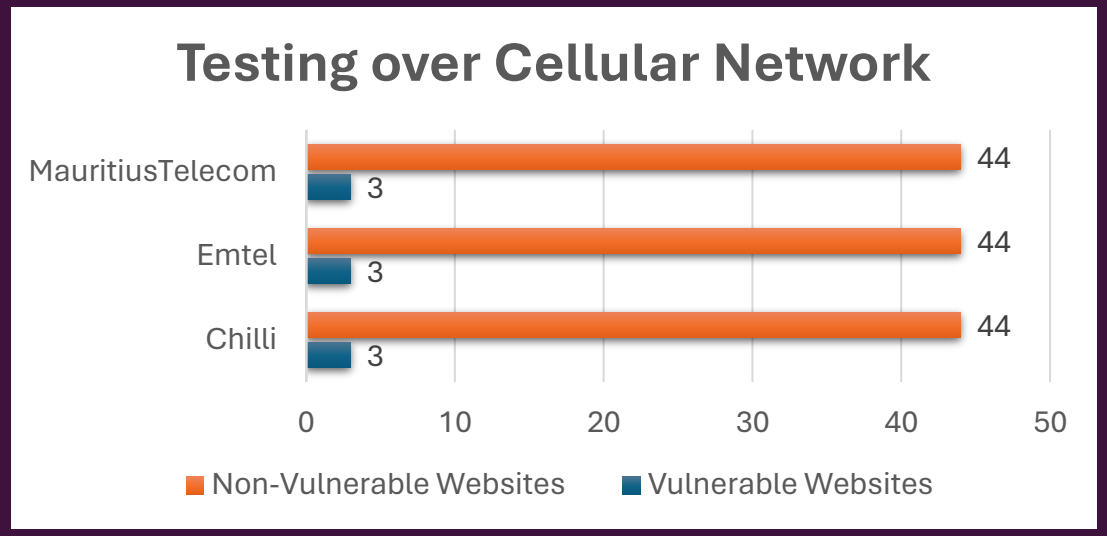
The Results

Mauritius IP ranges



6 out of 13 : Emtel-Mobile-BDR
7 out of 13: Emtel-Mobile-ASN

Most Popular Websites In Mauritius



Tested with 3 different ISPs
For each, 3 out of 47 Failed