

TFTP

You may have recently received a letter and/or email from Sunrise explaining that we have been notified that a device on your network has a vulnerability known as an open TFTP vulnerability. If you have received such a communication from us, please follow the advice given on this page to resolve the issue.

Overview

TFTP is a service that allows for other devices on a network to remotely access files and folders on a device running the service without entering in login credentials. This service is designed only to be used on a small local network, such as your home, but when exposed to the wider Internet it can be misused by third parties to commit abuse.

What has happened?

We work with a number of not-for-profit organisations across security sectors that collate information on devices across the Internet that appear to be compromised or misconfigured. This means that your compromised or misconfigured device is publicly accessible on the Internet, and therefore the scanning that is performed by these organisations is not within your private network.

We suspect a device connected to your home network may have an open TFTP vulnerability. For more information on these reports please visit tftpscan.shadowserver.org

If the settings are left open they can be exploited to steal personal information and unwittingly participate in malicious activities, for example a Distributed Denial of Service (DDoS) attack.

It is therefore important that you follow the advice in this article.

Note: This article is intended to provide advice. Sunrise is not responsible for any issues encountered in the course of resolving the issue and is not able to provide any technical support for such problems.

How can the issue be fixed?

An open TFTP vulnerability can be resolved by configuring your firewall to block UDP port 69.

It is worth noting that blocking this port will only stop traffic over this port leaving or entering your home network. Services within your home that use this port should continue to work as normal.

To close the vulnerable port:

- Access your Router configuration page
- Login with your username and password, default will be shown on the Router itself
- Select the Port Forwarding option
- Remove any rules that will keep port 69 open
- Select the Port Triggering option
- Remove any rules that will keep port 69 open

Ensure all devices on your network are protected by a firewall. It is important to check all your devices sit behind a firewall.

Internet Matters

Sunrise is a Co-Founder and Member of iBarry.ch: a not-for-profit organisation working with online safety experts to bring you all the information you need to help keep you and your children safe online.

For more information about iBarry, please visit <https://www.ibarry.ch/en/>