SNMP

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 Simple Network Management Protocol (SNMP) vulnerability. If you have received such a communication from us, please follow the advice given on this page to resolve the issue.

Overview

SNMP (Simple Network Management Protocol) is a method by which a device can be managed or accessed remotely on a computer network. An SNMP vulnerability is a security issue whereby a 3rd party can use this protocol to ultimately gain unauthorised access to your network/devices for malicious purposes, if the protocol is configured incorrectly.

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 a SNMP vulnerability.

For more information on these reports please visit snmpscan.shadowserver.org

If the settings are left open they can be exploited to 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?

The easiest way to deal with SNMP threats/vulnerabilities is to configure your firewall to block UDP ports 161 and 162.

It is worth noting that blocking these ports will only stop traffic over that port leaving or entering your home network. Services within your home that use ports 161 and 162 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 161 and 162 open
- Select the Port Triggering option
- Remove any rules that will keep port 161 and 162 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/