Cyber Snapshot

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

December 14, 2020
CS-08-2020

Default Configurations – Security & Certificates

OVERVIEW

Most internet-connected devices are designed to simplify setup. One such design is a default configuration. These default configurations are not meant for permanent use, as most are known, and the information is available to malicious actors online. To better secure your devices, it is important to review and change all factory-set default configurations.

EXAMPLES OF VULNERABLE DEFAULT CONFIGURATIONS

One example is using default usernames and passwords on devices and accounts utilized for IoT, networking, and security. Most of these credentials are publicly known and published online which allows attackers to harvest and exploit them. Using default configurations like this can nullify all security practices a company has implemented.

Another over-looked security configuration is default certificates supplied with some devices. For example, the FortiGate VPN Client, when operated under the default settings, does not verify if the user's certificate is specific to the FortiGate device, but only that the incoming certificate is valid from any Certificate Authority (CA). FortiGate advises users in their manual to change/update the default certificates, as these are important security objects used with verification and authentication. See https://kb.fortinet.com/kb/documentLink.do?externalID=FD49965.

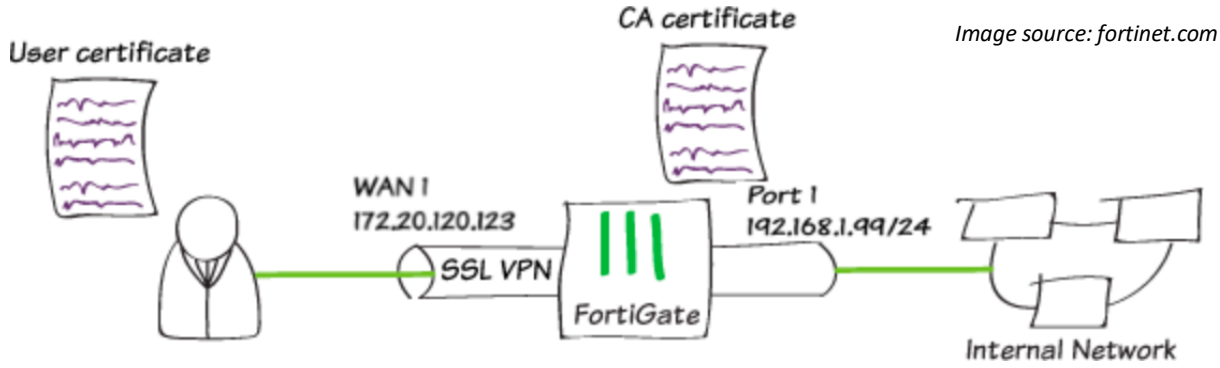

Image source: fortinet.com

ADDRESSING THE ISSUE

Most devices are designed to work straight out of the box, i.e., plug and play. This allows for an easy setup and use of the device. However, default configurations also make these devices vulnerable to attackers who know the default configurations and how to exploit them. Therefore, the MC3 recommends reviewing and updating security settings for all devices connected to networks. Users should review, update, and customize all security features of devices/software to meet their needs. Doing this will help ensure your data is kept secure and out of the hands of malicious actors.