Jason Lindsley
MIS 5211 – Introduction to Ethical Hacking
Analysis Report 2 – Scanning Exercise

Scan Results for Raspberry Pi - Volumio

Overview

Raspberry Pi devices are credit card-sized computers that are produced in the United Kingdom. They are intended to be used to promote affordable computer education in classrooms and developing countries. These devices run an operating system on a mini SD card and some models have up to four USB slots, a LAN network connection, and an HDMI display port. There are many open source projects and distros available that are easily flashed to these mini SD cards and enable many Internet connected applications. Many individuals use Rasperry Pi devices to create alternative solutions to expensive commercially branded Internet of Things (IoT) devices. In addition, Raspberry Pi is a popular hardware choice for entrepreneurs to rapidly develop cheap prototype IoT solutions that are not yet commercially available. I purchased a Raspberry Pi device to experiment with some of the open source projects and to get more experience with Linux operating systems. One of my first projects was to create a streaming audio player using a Volumio, an open source package that is easily installed onto Raspberry Pi.

Volumio

Volumio is a Debian Linux-based software distribution that is configured out of the box to enable high resolution network audio streaming (including via Apple's Airplay). Users can access the system through a web browser on a device connected to the same network. The web browser allows users to change configurations and stream audio. Once installed and connected to a network, audio streaming to speakers connected to the Raspberry Pi hardware is available without any additional configuration.

Security Risks

Open-source software such as Volumio, carries many inherent risks. These devices are made to be plug-and-play and therefore security is typically not prioritized in the design of the software. Therefore, open-source software can typically use generic privileged accounts, default passwords (non-complex), weak security configurations, non-essential OS software and services, exploitable operating system vulnerabilities, and more.

Nessus Scan Results

I performed a Basic Network Scan on my Rasperry Pi Volumio device using Nessus. The results included one High risk vulnerability and Two medium risk vulnerabilities related to the Samba daemon. Samba, derived from the protocol Server Message Block (SMB), allows file and print sharing between computers running Microsoft Windows and Unix-like systems (e.g. Linux, AIX, Solaris, etc.). Based on additional research, the Samba service is open in Volumio to enable users to mount shared network storage to the device to play audio files from remote devices. I stream my audio files from internet services such as Spotify and I do not require the ability to mount network storage. The following is a summary of the vulnerabilities that were noted and the recommendation to remove the Samba in the Debian version of Linux:

Jason Lindsley
MIS 5211 – Introduction to Ethical Hacking
Analysis Report 2 – Scanning Exercise

Vulnerability	Risk	CVE Reference	Risk Rating	Recommendation*
SMB Shares Unprivileged Access	Network storage shares can be accessed using a NULL session and may allow attacker to read/write data on the remote host.	CVE-1999-0519, CVE-1999-0520	High	Remove the entire Samba package, including configuration files, with the following command: - sudo apt-get purge Samba It is recommended to make a backup copy of the micro SD card prior to disabling the Samba service in the event that the change disrupts operations completely.
SMB Guest Account Local User Access	The remote host is running the Samba daemon and is configured to allow access via a guest user using a random account.	CVE-1999-0505	Medium	
SMB Signing Disabled	Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.	Not Available	Medium	

Other Considerations

The Nessus "Basic Network Scan" scans for known OS vulnerabilities. It does not typically check for application specific security weaknesses such as generic accounts and non-complex default passwords. Based on additional investigation, I found that Volumio uses some simple default passwords for root and other privileged accounts. Therefore, the software is inherently vulnerable to other attacks such as the recent Mirai vulnerability that exploits IoT devices to serve as "zombies" in botnet denial of service attacks. Therefore, it is also recommended to change the default passwords and continually update the Volumio OS software.

Remediation Results

After performing precautionary backups, I tested the following remediation activities to determine the impacts it would have, if any, on Volumio's functionality in my environment:

- Disable Samba service on the Debian Linux OS
- Change default passwords for privileged accounts (i.e. root & volumio) to complex passwords

The Volumio software continued to function as I intended it after these changes. I re-ran a Basic Network Scan using Nessus and the results were positive. The one High risk finding and two Medium risk findings were no longer listed in the results of the scan.

This exercise was a great example of how non-essential software and services can create vulnerabilities that are easily addressed through system hardening activities such as configuration changes and uninstalling non-essential software.