sohsatoh / **gist:02699fbbdff90e6c2078b508f830022b** Secret

Last active 2 days ago

Yamaha SR-B30A BLE Unauthorized Control Vulnerability

gistfile1.md

Yamaha SR-B30A BLE Unauthorized Control Vulnerability

Summary

The Yamaha SR-B30A sound bar allows unauthenticated Bluetooth Low Energy (BLE) connections to its control interface used by the official Sound Bar Remote mobile application.

An attacker within BLE radio range can connect to the device without authentication and send control commands.

Affected Product

Vendor: Yamaha

Product: SR-B30A Sound Bar

Device Firmware: 1.03

The issue exists in the device firmware. The official mobile application (Sound Bar Remote v2.40) communicates with the device over the affected BLE interface.

Vulnerability Details

The SR-B30A exposes a Bluetooth Low Energy (BLE) control interface used by the Sound Bar Remote mobile application.

The device accepts BLE connections without requiring:

- authentication
- authorization

Because of this behavior, any nearby BLE device can establish a connection and interact with the control interface.

Once connected, the attacker can:

- send device control commands
- change audio volume
- maintain a persistent BLE connection

Impact

Denial of Service

An attacker can maintain a persistent BLE connection which prevents legitimate users from connecting using the official Sound Bar Remote application.

Unauthorized Device Control

The attacker can send control commands to the device such as volume adjustments or other operational commands.

This may cause unintended device behavior in the physical environment.

Attack Requirements

- Attacker must be within Bluetooth Low Energy radio range (~10–30 meters)
- No authentication or pairing is required

Attack Scenario

1. Attacker scans for nearby BLE devices

2. Attacker connects to the SR-B30A BLE service
3. Attacker maintains the connection to block legitimate control
4. Attacker sends device control commands

Vendor Disclosure

The vulnerability was reported to Yamaha. The vendor has indicated that no fix will be provided.

Discoverer

Soh Satoh

CVE

CVE-2026-37100