



## Airmedia - Nessus Vulnerability Scanner False Positive Mitigation Guideline - Airplay

Product - AM101

Feature - Airplay Service

Firmware - 2.6.x.x to 2.8.x.x

Date - 24<sup>th</sup> September 2018

**Vulnerability Reported by Nessus Scanner:**

Nessus vulnerability scanners report Airplay library with a build number of 12H523 isopen to multiple vulnerabilities.

Nessus Vulnerability title	CVE associated	Port
Apple TV < 11.2.6 Telugu Character Handling Remote Memory Corruption Vulnerability	CVE-2018-4124	7000
Apple TV < 11.3 Multiple Vulnerabilities	CVE-2018-4155, CVE-2018-4142, CVE-2018-4167	
Apple TV < 11.4 Multiple Vulnerabilities	CVE-2018-4243, CVE-2018-4237, CVE-2018-4235, CVE-2018-4240, CVE-2018-4224, CVE-2018-4223, CVE-2018-4198, CVE-2018-4232, CVE-2018-4192, CVE-2018-4214, CVE-2018-4204, CVE-2018-4246, CVE-2018-4200, CVE-2018-4201, CVE-2018-4218, CVE-2018-4233, CVE-2018-4188, CVE-2018-4199, CVE-2018-4190, CVE-2018-4222,	
Apple TV < 11.4.1 Multiple Vulnerabilities	CVE-2018-4293, CVE-2018-4282, CVE-2018-4280, CVE-2018-4248, CVE-2018-4277, CVE-2018-4270, CVE-2018-4278, CVE-2018-4284, CVE-2018-4266, CVE-2018-4261, CVE-2018-4262, CVE-2018-4263, CVE-2018-4264, CVE-2018-4265, CVE-2018-4267, CVE-2018-4272, CVE-2018-4271, CVE-2018-4273,	
Apple TV <= 7.2.2 Bluetooth Remote Code Execution (BlueBorne)	No Bluetooth on AirMedia range of devices	
Apple TV < 11.1 Multiple Vulnerabilities	CVE-2017-13849, CVE-2017-13799, CVE-2017-13852, CVE-2017-13804, CVE-2017-13783, CVE-2017-13784, CVE-2017-13785, CVE-2017-13788, CVE-2017-13791, CVE-2017-13792, CVE-2017-13793, CVE-2017-13794, CVE-2017-13795, CVE-2017-13796, CVE-2017-13797, CVE-2017-13798, CVE-2017-13802, CVE-2017-13803, CVE-2017-13077, CVE-2017-13078, CVE-2017-13080,	
Apple TV < 11.2 Multiple Vulnerabilities	CVE-2017-7164, CVE-2017-7172, CVE-2017-7171, CVE-2017-7162, CVE-2017-13861, CVE-2017-13904, CVE-2017-5754, CVE-2017-13862, CVE-2017-13867, CVE-2017-13876, CVE-2017-7173, CVE-2017-13855, CVE-2017-13865, CVE-2017-13868, CVE-2017-13869, CVE-2017-7154, CVE-2017-13885, CVE-2017-7165, E-2017-13884 CVE-2017-7153, CVE-2017-7156, CVE-2017-7157, CVE-2017-13856, CVE-2017-13870, CVE-2017-7160, CVE-2017-13866, CVE-2017-13080	

### Why does Nessus find this as an issue?

The AirMedia device advertises specific AppleTV version numbers i.e 12H523 in order ensure compatibility with different devices.

None of these vulnerabilities actually applies to the library employed in AirMedia devices, but are picked up by security scanner as “vulnerable” because the scanner fingerprints AppleTV version number that is being broadcasted.

Thus, in summary, these vulnerabilities found by the Nessus scanner are false positives and apply only to AppleTVs with relevant versions numbers, but not to the specific Library that AirMedia uses.

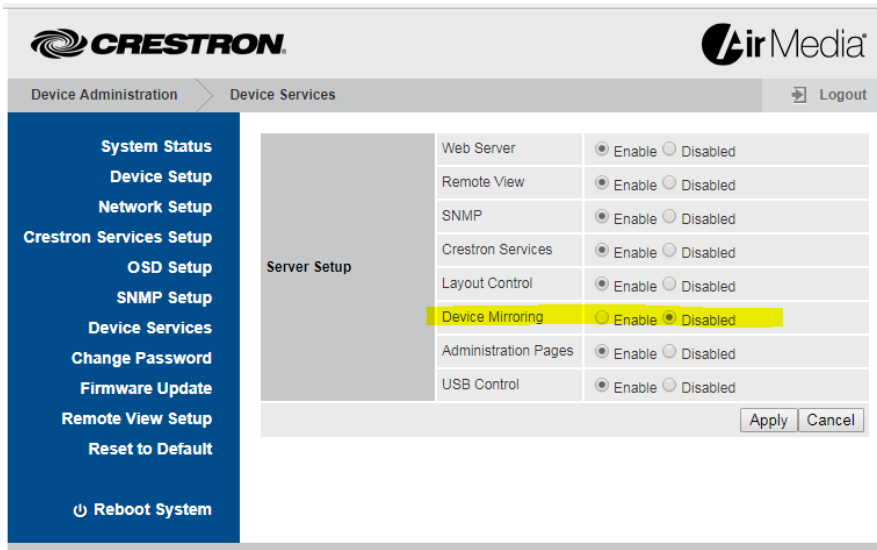
### Port Number Affected : 7000

### Work Around:

No actions needed since it is a false positive.

### Disabling Airplay

1. Navigate to device “Services Page”.
2. Airplay can be turned off by disabling Device mirroring functionality as shown below.



3. Device mirroring disables only Airplay functionality of AirMedia Devices, the windows/mac application still works with airplay disabled.