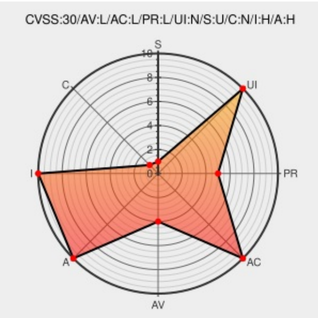
CVE-2018-14987

Published on: 12/28/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:43 PM UTC

CVE-2018-14987

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mxq Tv Box from Mxq Project contain the following vulnerability:

The MXQ TV Box 4.4.2 Android device with a build fingerprint of MBX/m201_N/m201_N:4.4.2/KOT49H/20160106:user/test-keys contains the Android framework with a package name of android (versionCode=19, versionName=4.4.2-20170213) that dynamically registers a broadcast receiver app component named com.android.server.MasterClearReceiver instead of statically registering it in the AndroidManifest.xml file of the core Android package, as done in Android Open Source Project (AOSP) code for Android 4.4.2. The dynamic-registration of the MasterClearReceiver broadcast receiver app component is not protected with the android.permission.MASTER_CLEAR permission during registration, so any app co-located on the device, even those without any permissions, can programmatically initiate a factory reset of the device. A factory reset will remove all user data and apps from the device. This will result in the loss of any data that have not been backed up or synced externally. The capability to perform a factory reset is not directly available to third-party apps (those that the user installs themselves with the exception of enabled Mobile Device Management (MDM) apps), although this capability can be obtained by leveraging an unprotected app component of core Android process.

CVE-2018-14987 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	HIGH

CVSS2 Score: 5.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	COMPLETE

CVE References

Description	Tags	Link
Page not found | Kryptowire	Third Party Advisory www.kryptowire.com application/pdf Inactive Link Not Archived	MISC www.kryptowire.com/portal/wp-content/uploads/2018/12/DEFCON-26-Johnson-and-Stavrou-Vulnerable-Out-of-the-Box-An-Eval-of-Android-Carrier-Devices-WP-Updated.pdf
Kryptowire Provides Details on DEFCON 2018 Presentation: Vulnerable Out of the Box - An Evaluation of Android Carrier Devices - Kryptowire	Third Party Advisory www.kryptowire.com text/html	MISC www.kryptowire.com/portal/android-firmware-defcon-2018/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Mxq Project	Mxq Tv Box	-	All	All	All
Hardware	Mxq Project	Mxq Tv Box	-	All	All	All
Operating System	Mxq Project	Mxq Tv Box Firmware	4.4.2	All	All	All
Operating System	Mxq Project	Mxq Tv Box Firmware	4.4.2	All	All	All

cpe:2.3:h:mxq_project:mxq_tv_box:-:*:*:*:*:*:*:

cpe:2.3:h:mxq_project:mxq_tv_box:-:*:*:*:*:*:*:

cpe:2.3:o:mxq_project:mxq_tv_box_firmware:4.4.2:*:*:*:*:*:*:

cpe:2.3:o:mxq_project:mxq_tv_box_firmware:4.4.2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE