

[SHADOWED b/529641895] [BTS] New Inquiry: <BFX-AT100>/< VBMeta test key>

+1 Hotlists (6) Mark as Duplicate

Comments (8) Dependencies Duplicates (0) Blocking Resources (6)

In Progress Process P1 +

STATUS UPDATE No update yet. Edit

DESCRIPTION Edit

Cathy Liu created issue #1

Jun 30, 2026 01:38PM

== Required Information ==

Build fingerprint: SKB/BFXAT100/BFX-AT100:12/STTC.220724.001/15.561.128-20260611:user/release-keys

AFAP link: (If available) https://partner.android.com/firmwares/buildfingerprints?bf=SKB%2FBFX_AT100%2FBFX-AT100:12%2FSTTC.220724.001%2F15.561.128-20260611:user%2Frelease-keys&bid=&bs=&a=1995079395

Failure type (PHA, Patch analyzer, INFO, etc): INFO VBMeta test key

Description of failure: Two BTS warnings will be changed to alert at 2026-08-06. 1.vbmeta signed with VBMeta test key 2.recovery signed with VBMeta test key

Both partition 'vbmeta' and 'recovery' are signed with a publicly known VBMeta test key '22de3994532196f61c039e90260d78a93a4c57362c7e789be928036e80b77c8c', causing the device's boot integrity to be broken.

The device passes BTS and all certification tests. However the bootloader contains a fixed AVB root public key. Replacing the AVB key causes Verified Boot failure and the device continuously reboots during boot.

Related CVE (if applicable): N/A

== Justification ==

Why the ticket being created: This device is a legacy OTT STB based on Amlogic S905X2 and has been commercially deployed for several years.

The AVB root public key is embedded in the bootloader and cannot be updated through OTA. Replacing the AVB key results in Verified Boot failure and device bootloop.

Because deployed devices cannot update the bootloader trust key, changing the AVB key is not technically feasible for field devices.

Reporter

cathy_liu3@pegatron.c...

Type

Process

Priority

P1

Severity

S2

Status

In Progress (Accepted)

Mark fixed

Access

Default access View

Expanded Access

Assignee

cathy_liu3@pegatron.c...

Verifier

Collaborators

android-partner-prodops-bars

Add Add me

CC

almoguera@google.com

android-bug-triage@google.co

ape-prodops-sbf@google.com

cathy_liu@pegatron.corp-part

cathy_liu3@pegatron.corp-pa

wshen@google.com

Add Un-CC me

We request a waiver / exception for the AVB test key warning for this legacy device.

== Additional Information and Justification==

Why the ticket being created:

Additional Info: Device status: Commercial product in maintenance stage (EOL). Chipset: Amlogic S905X2 Android version: Android 12

Replacing AVB key has been tested but causes boot failure because the bootloader trust key is fixed. Therefore the AVB key cannot be changed on deployed devices.

COMMENTS

All comments

↓ Oldest first



almoguera@google.com <almoguera@google.com> [#2](#)

Jun 30, 2026 04:37PM

Hi team. Can you please take a quick look and confirm that you are the right assignee to handle this request? If not, please re-assign to a more appropriate team member or assign back to android-bug-triage@google.com if this issue was incorrectly routed to your team. Thanks!



almoguera@google.com <almoguera@google.com> [#3](#)

Jun 30, 2026 04:38PM

Reassigned to [ape-prodops-sbf@google.com](#).

hotnachos: shadow -> 769877



android-partner-prodops-barscanner@prod.google.com
<android-partner-prodops-barscanner@prod.google.com> [#4](#)

Jun 30, 2026 04:38PM

A Google-internal buganizer issue has been created: [b/529641895](#). We will provide updates here as they are made in that issue.



android-partner-prodops-barscanner@prod.google.com
<android-partner-prodops-barscanner@prod.google.com> [#5](#)

Jun 30, 2026 04:39PM

Reassigned to [bugjuggler@google.com](#).

Bugjuggler: [b/529641895](#) -> [almoguera@google.com](#)

Code Changes	--	Add	
Pending Code Changes	--		
ETA	--		
Asgd to Privacy	--		
Bug Weight	--		
Chase Source	--		▼
Chase Status	--		
Docs: 1-pager	--		
Expected Impact	--		▼
FKBB	--		
GAR Level	--	Edit	
LKGB	--		
ML Component Suggestion	--	Add	
ML Duplicate Suggestion	--	Add	
Privacy due date	--		
Project Status	--		▼
Regressed From	--	Edit	
Regressed Metric Name	--		
Regression	--		▼
Regression ATP Config Name	--		
Regression Test Name	--		



bugjuggler@prod.google.com <bugjuggler@prod.google.com> #6

Jun 30, 2026 04:40PM

Accepted by bugjuggler@google.com.

Hi. I've received your bug and will wait for [b/529641895](#) to be resolved and then assign the bug to almoguera.



jeanhazel@google.com <jeanhazel@google.com> #7

Jun 30, 2026 09:48PM

MESSAGE FROM THE ENGINEERING TEAM

Hello Pegatron Team, Thank you for your submission, we will start our investigation immediately.



johnangelop@google.com <johnangelop@google.com> #8

Jul 1, 2026 06:51AM

Assigned to cathy_liu3@pegatron.corp-partner.google.com.

Message from Engineering Team



Hi Pegatron Team - This is a True Positive. The current build [↗SKB/BFX_AT100/BFX-AT100:12/STTC.220724.001/15.561.128-20260611:user/release-keys](#) seems to have VBMeta signed with known AOSP test keys instead of private production keys as detailed below.

Partition Name	VBMeta test key	Action item
vbmeta	22de3994532196f61c039e90260d78a93a4c57362c7e789be928036e80b77c8c	AOSP test key must be re-signed with the OEM release key
recovery	22de3994532196f61c039e90260d78a93a4c57362c7e789be928036e80b77c8c	AOSP test key must be re-signed with the OEM release key

As per the [↗Partner Security Advisory—2025-05 \(CVE-2025-48613 VBMeta Test Key\)](#) guidelines, partners must ensure that their VBMeta data structure is signed with their OEM release key and NOT an AOSP test key. Any data structures identified as being signed with AOSP test keys must be re-signed with the OEM release key. **Android Security will require these changes for compliance with the 2026-03-05 SPL.**

Why the ticket being created: This device is a legacy OTT STB based on Amlogic S905X2 and has been commercially deployed for several years.
The AVB root public key is embedded in the bootloader and cannot be updated through OTA. Replacing the AVB key results in Verified Boot failure and device bootloop.

Root Cause	--	Edit
Security Ranking Score	--	
SysSW-Bug-DRI	--	
SysSW-Bug-Src	--	
Themes	--	
Visual Bug Capture	--	
CarrierConfig App Name	--	
CarrierConfig Certificate SHA256	--	
CarrierConfig Package Names	-- Add	
CarrierConfig XML File Name	--	
Dependency Commitment	--	
Execution Status	--	
FR Status	Pre-PRD	
ID for APA	--	
ID for APA Date	--	
PTE Functional Area	-- Edit	
PTE Product Line	-- Edit	
SLO Anchor Date	--	
Found In	--	

Because deployed devices cannot update the bootloader trust key, changing the AVB key is not technically feasible for field devices.

We request a waiver / exception for the AVB test key warning for this legacy device.

Replacing AVB key has been tested but causes boot failure because the bootloader trust key is fixed. Therefore the AVB key cannot be changed on deployed devices.

A potential workaround, which has been successfully explored by at least one partner with their SoC vendor, is to modify the Android Bootloader (ABL). The ABL can be updated to report the old, exposed key to KeyMaster/KeyMint while verifying the image with a new production key. This would allow for migration from the vulnerable key without requiring a factory reset.

Please let us know if you require any additional information.



Cathy Liu <cathy_liu3@pegatron.corp-partner.google.com>

Jul 1, 2026 09:25AM

Accepted by  *cathy_liu3@pegatron.corp-partner.google.com*.

Add

Targeted To

--

Add

Verified In

--

Add

In Prod



Show 32 additional fields

