Instantly share code, notes, and snippets.

throwaway96 / **crashd.md**

Last active 1 hour ago

Star | Code | Revisions 93 | Stars 219 | Forks 4

crashd instructions

crashd.md

News

READ THIS FIRST: Patched firmware released (2024-01-03)

> Important
>
> Production firmware that removes the vulnerability has been released for some models.

If you have a model with one of these OTAID, you should assume it is patched if you have the firmware version listed below or newer. Newer versions that are confirmed patched are listed for convenience.

Patched firmware versions known to have been released:

- W23O - 03.30.60 (also 03.30.70)
- W22H - 04.40.75 (also 04.40.80)
- W22O - 04.40.90

Note: There are many models that we are unable to provide patch information for, but you may be able to help. Please contact us via Discord if you have a TV with an OTAID containing W22K, W23K, or W23L.

Warning: crashd about to be patched (2023-12-28)

LG is working on firmware that removes `cloudupload`, which contains the underlying vulnerability exploited in this guide. They appear to be planning to include this fix in webOS 7.4.0 and 8.3.0, but they will likely eventually apply it to all currently supported webOS versions.

Firmware versions known to be patched:

- W23H, W23O, W23P - 03.30.60
- W22H, W22P, C22H - 04.40.75
- W22H webOS 8 upgrade - 13.30.13
- W22L - 04.40.85
- W22O - 04.40.80
- W21K, W21O - 03.40.85
- W21P - 03.40.80

Obviously, if you want to root your TV, **don't update**.

Note: Alternative to crashd (2023-10-30)

If for whatever reason you are unable to use the crashd exploit but still want to root your TV, **do not install any new firmware updates**. LG has started rolling out patches for another vulnerability. Further details are not yet available.

Note: 2023 models (2023-03-29)

This guide will work on 2023 models. *If you have an FHD (1080p; model number should contain "LR"), QNED or NANO (nanocell) 2023 LG TV, please contact us on Discord.*

Introduction

THIS ONLY WORKS ON webOS 4+!

This guide explains how to root an LG TV using a vulnerability in `crashd`. It works on webOS 4 and above but ***will be patched soon***. This means that if your TV is *not* running at least webOS 4.0 (i.e., it is a 2018 model or newer), it is *not vulnerable*. If you are running an older version of webOS, your options are:

- RootMyTV — Firmware released since roughly mid-2022 is probably not vulnerable. This document lists vulnerable versions for certain SoCs.
- GetMeIn — Only works on certain SoCs (maybe just Realtek and LX). I'm not sure which webOS versions are vulnerable, but I have seen it work on webOS 2.2 and 3.4.2. GetMeIn modifies `start-devmode.sh` , which will result in apps being removed on webOS versions that have RootMyTV patched. You will have to modify `jail_app.conf` to get access to `/dev/mem` .
- modifying debugstatus in the NVM — Involves opening your TV and directly accessing the an EEPROM IC. After enabling debug mode, you'll need to spawn a root shell and use it to permanently enable developer mode and install/elevate Homebrew Channel.

Please don't ask me whether a specific firmware version is vulnerable. First, I probably don't know. Second, I'll update this document if LG starts releasing patched firmware. **See the News section above.** Also note that a firmware version without the corresponding model number is practically meaningless.

It is recommended that anyone attempting this procedure do their own research in order to understand how the process works. In general, unless you understand exactly why you're doing something, you shouldn't do it. While there is relatively low risk of permanent damage to your TV, **you're ultimately responsible if anything goes wrong.**

This guide assumes you're working from a desktop PC, although the same process can be performed from a smartphone. Where PuTTY is used in this guide, any telnet client will work. You can also use LG's CLI tools or any SSH client instead of the Dev Manager program, although complete instructions for those are not (yet) provided. (There are some hints, though.)

If you have trouble with any of these steps, the solution is probably somewhere in this document. Basically everything that can go wrong is discussed in the FAQ section below (in particular the Rooting questions). If you're going to ask for help, make sure you know *both* the webOS *and* firmware/"software" versions. Also, if you are going to ask about a specific firmware version, **please provide an OTAID** so people can know what you're talking about.

General Tips

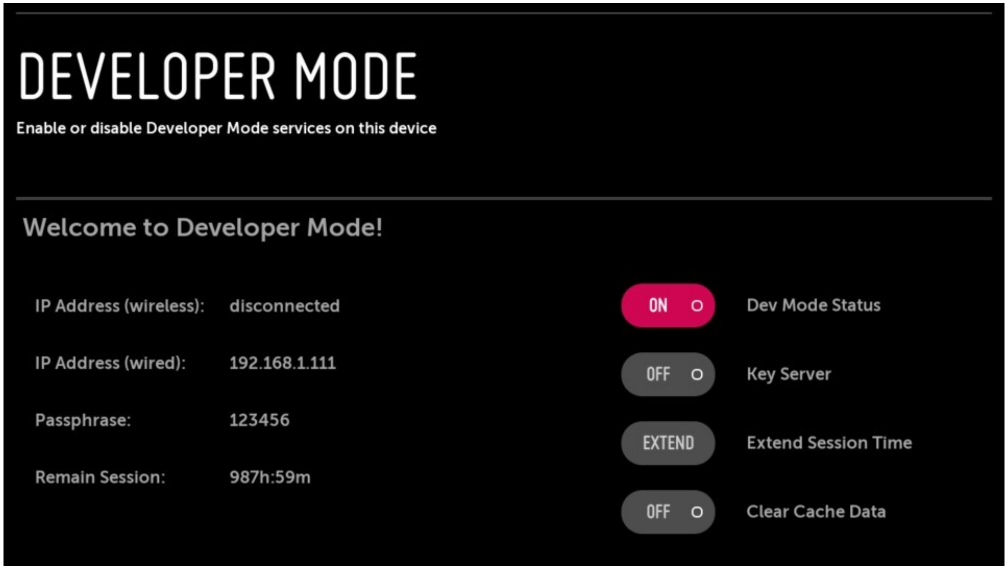
- **This will only work on webOS 4+.**
- You can copy and paste commands into recent versions of Dev Manager.

- For many commands (e.g., `touch`, `mkdir`, `rm`), there will be no output if the command is successful. The prompt (`>`) in Dev Manager will be blue after a successful command and red after an error.
- The commands involved in this process should complete more or less instantly. If it hasn't completed after 30 seconds, cancel it and try again.
- Use the latest version of Dev Manager and Homebrew Channel.
- Make sure Quick Start+ is disabled for rebooting to be effective.
- OLEDs may have to be unplugged to properly reboot, as they can remain on for a while despite appearing to be off.

Steps

0. Read this guide. Seriously. Especially the introduction above. Check the news at the top for recent changes that may be relevant to your TV. If you have issues, look at the tips and FAQ before asking any questions. If your TV runs webOS 1, 2, or 3, *stop now* and read the introduction.

1. Enable Developer Mode on the TV: See this guide from LG. If you have trouble (e.g., not getting the prompt to sign in), try rebooting. (You can ignore the "UPDATE NOTICE" about needing to install webOS TV CLI v1.12.4 or later.) A reboot is required after setting Dev Mode Status to ON. The Developer Mode app should look something like this:



DEVELOPER MODE

Enable or disable Developer Mode services on this device

Welcome to Developer Mode!

IP Address (wireless): disconnected

IP Address (wired): 192.168.1.111

Passphrase: 123456

Remain Session: 987h:59m

ON Dev Mode Status

OFF Key Server

EXTEND Extend Session Time

OFF Clear Cache Data

2. Download and install the following software on your PC:

   - WebOS-Dev-Manager - Use the latest version (1.12.1 as of 2023-12-28), or you will have problems.

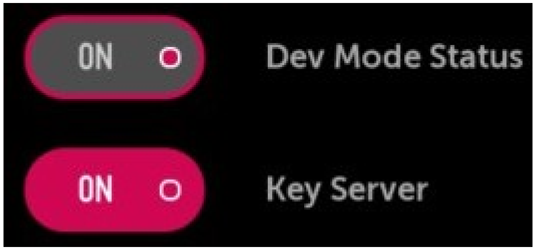
   - PuTTY

   Download the following file to your PC:

   - Homebrew Channel IPK - Use the latest version (0.6.3 as of 2023-12-28).

3. Disable Quick Start+ on the TV. This is in the menu, but its exact location depends on the webOS version. For example, on webOS 5, after pressing the menu button on the remote, it can be found in All Settings > General > Additional Settings. On webOS 6 and 7, it is under All Settings > General > Devices > TV Management.

4. Reboot the TV (e.g., by turning it off and then back on) again. This is in addition to the reboot required when enabling developer mode. *Make sure Quick Start+ is disabled!*
   Note: If you have an OLED TV, it may stay on for a while (to run the Pixel Refresher) despite appearing to be off. Thus, when you turn it back on, it won't have actually rebooted. You can unplug it to be sure it's off.

5. In the LG Developer Mode app, enable the Key Server. It should look like this:
   
   ON ○ Dev Mode Status
   ON ○ Key Server

   Note that the key server only needs to be enabled while you are connecting for the first time. It will be automatically disabled on reboot.

6. In Dev Manager, perform these steps:
   a. Click "+ Add Device"
   b. Enter IP address of your TV in "Host Address" field
   c. Enter passphrase displayed on LG Developer Mode app in "Passphrase" field
   d. Keep other settings at default, click "Add" (troubleshooting errors)
   e. Click "Install" in the top right corner
   f. Choose Homebrew Channel IPK
   g. Make sure Homebrew Channel is installed on your TV
   h. Click on "Terminal"
   i. Use `jailpatch.sh` to generate an old `jail_app.conf` with a valid signature:

```
curl -L -o /tmp/jailpatch.sh https://raw.githubusercontent.com/throwaway96/in
```

Make sure the output says `verification of current conf successful` before continuing.

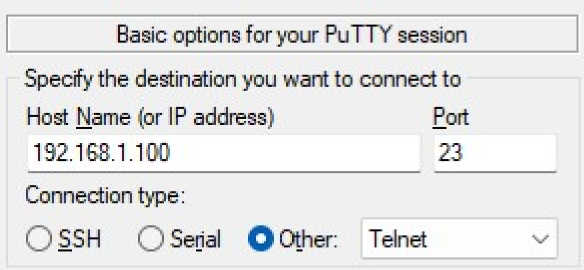
7. Reboot the TV (e.g., by turning it off and then back on) for a third time. *Make sure Quick Start+ is disabled!*

8. In Dev Manager, go to "Terminal" and input this command **EXACTLY**, then press enter:

```
touch /var/log/crashd/"x;telnetd -l sh"
```

Note: The character after the dash is a lowercase L, not a one.
If you get an error like `sh: touch: not found`, just repeat the command. When successful there should be no output.
If you get a "Permission denied" error, you probably didn't complete the previous steps regarding `jail_app.conf` correctly or did not reboot afterward.

9. In PuTTY perform these steps:
a. Type your TV's IP address in "Host Name" field
b. Validate that "Other" and "Telnet" are selected under "Connection type"



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.100

Port: 23

Connection type: ○ SSH ○ Serial ● Other: Telnet

Note: The default port of 23 is correct.
c. Open the telnet connection to your TV
d. Execute this to give root permissions to Homebrew Channel (you can paste into PuTTY by right clicking or pressing Shift+Insert):

```
/media/developer/apps/usr/palm/services/org.webosbrew.hbchannel.service/eleva
```

e. Execute this command to ensure developer mode never expires:

```
rm -rf /var/luna/preferences/devmode_enabled && mkdir -p /var/luna/preference
```

f. If you have used RootMyTV before (even unsuccessfully), execute this command to remove leftover files:

```
rm /var/lib/webosbrew/startup.sh /mnt/lg/cmn_data/wam/extra_conf.sh
```

10. Uninstall developer mode app from TV home menu.
    WARNING: Do NOT reinstall the LG Developer Mode app while your TV is rooted!

11. Power off your TV. *Make sure Quick Start+ is disabled!*
    Note: If an "Install Homebrew Channel" prompt appears (unlikely), don't choose "yes".

12. After restart, confirm that "Root status" in Homebrew Channel is "ok"

13. Turn on SSH in Homebrew Channel and restart
    Note: The default SSH password is `alpine`.

14. Enjoy your rooted TV!
    Note: If you want to block update notifications, you'll need to block certain domains.

Based on instructions by Shadow0304

If this guide helped you, please donate to support further development.

Notes

Authentication

The default root password (for SSH/SFTP) is `alpine`. Installing a public key for SSH authentication is recommended and will disable the default password. (The default password is not set on boot when `/home/root/.ssh/authorized_keys` exists.) This can be accomplished with the following commands:

```
mkdir -p /home/root/.ssh
chmod 700 /home/root/.ssh
echo '<key>' > /home/root/.ssh/authorized_keys
chmod 600 /home/root/.ssh/authorized_keys
```

Replace `<key>` with your key. It will look something like `ssh-rsa LongBase64String== comment`. See this guide for more information on setting up public key SSH authentication.

Homebrew Channel Version

Make sure you're using the latest version of Homebrew Channel (currently 0.6.3).

Versions

*Note: The webOS version is **not** the same as the firmware version.*

webOS versions

The TV models for each year all run the same major version of webOS. It is not possible to update from one major version to another, with a few exceptions. Note that webOS 3.0 and 3.5 are separate "major" versions despite having the same leading digit. This is also true for webOS 4.0 and 4.5.

Year	Version	Codename
2014	1.x	`afro`
2015	2.x	`beehive`
2016	3.0–3.4	`dreadlocks`
2017	3.5–3.9	`dreadlocks2`
2018	4.0–4.4	`goldilocks`
2019	4.5–4.9	`goldilocks2`
2020	5.x	`jhericurl`
2021	6.x	`kisscurl`
2022	7.x (22)	`mullet`
2023	8.x (23)	`number1`

Each major version has a codename that is a hairstyle. Each minor version has a codename that is a national park (or similar). The full codename of webOS 4.5, for example, is `goldilocks2-grandcanyon` .

With webOS 7, LG added a marketing name of "webOS 22", with the 22 indicating the year (2022). The webOS 8/23 situation is similar.

Firmware versions

The firmware version is often called "software version". Firmware versions look like `03.44.55`, with each of the three components being zero-padded to two digits. Production firmware versions all have a first component of at least 03, as lower numbers are reserved for testing.

FAQ

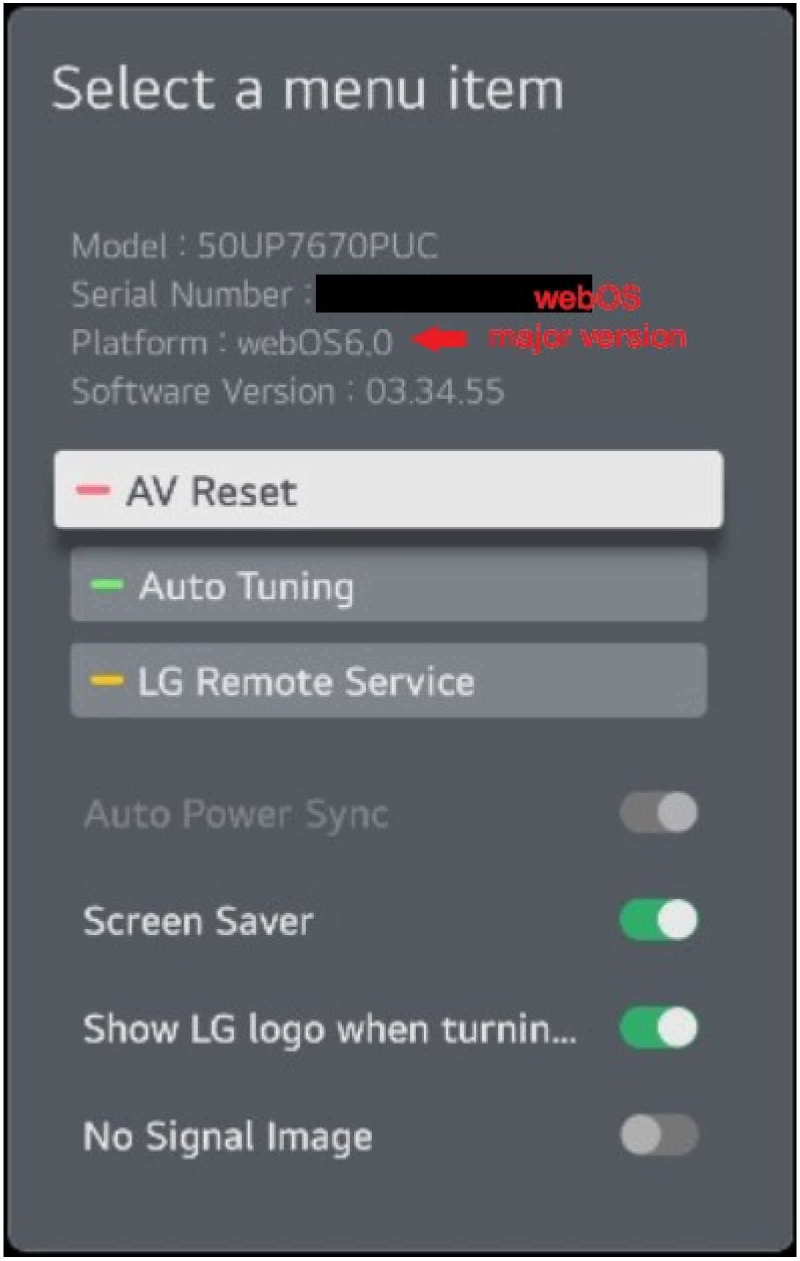
General

How do I know what version of webOS I am running?

This information can be found in the menu (accessed by pressing the button with a gear on the remote). The exact location within the menu varies across webOS versions.

The firmware and webOS versions are shown in the Host Diagnostics (HostDiag) screen. I have written instructions for entering HostDiag.

You also may be able to find the webOS major version by pressing the mute button three times rapidly. This is an example on a webOS 6 TV:



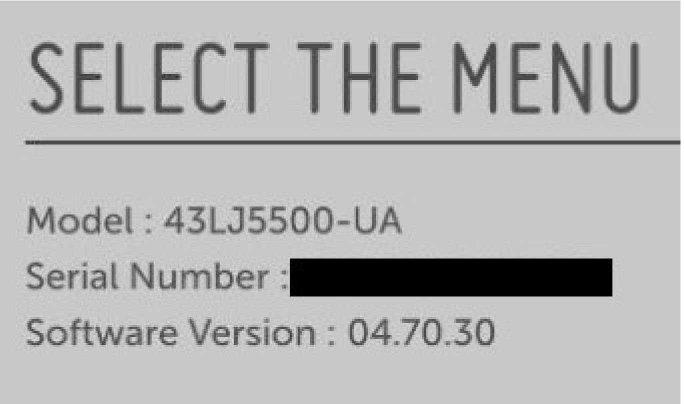
Select a menu item

Model : 50UP7670PUC
Serial Number : [redacted]
Platform : webOS6.0
Software Version : 03.34.55

webOS major version

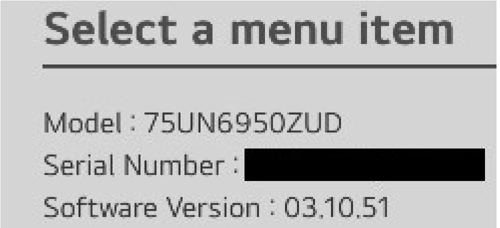
Note that the firmware version and model number are also shown. On webOS 7, this window looks similar but lacks the "Platform" field.

However, on other webOS versions including 3.5, 4.0, and 5, only the firmware version is shown:



SELECT THE MENU

Model : 43LJ5500-UA
Serial Number : [redacted]
Software Version : 04.70.30

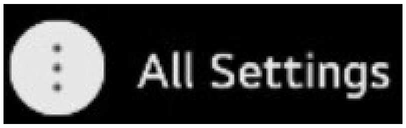


Select a menu item

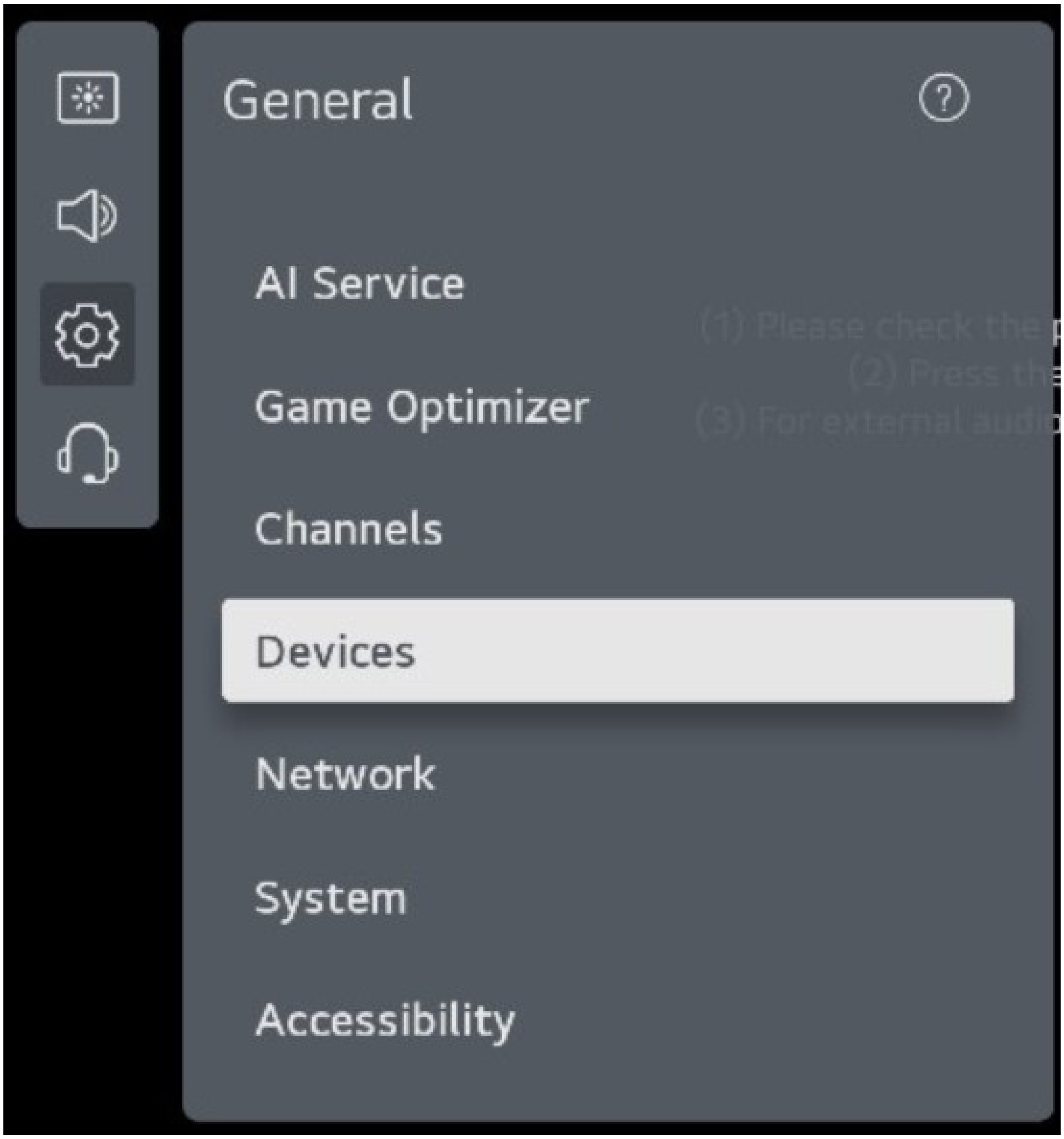
Model : 75UN6950ZUD
Serial Number : [redacted]
Software Version : 03.10.51

webOS 6 and 7

To find the version number through the menu on webOS 6 or 7, first press the menu button on the remote, then choose "All Settings":



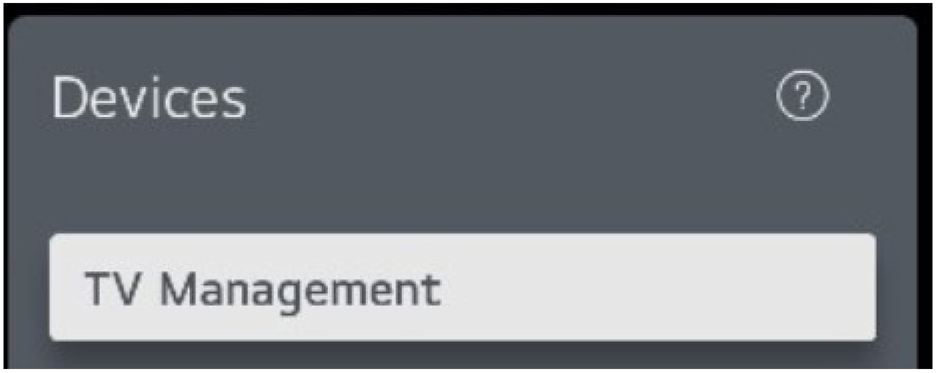
Next, choose "Devices" under "General":

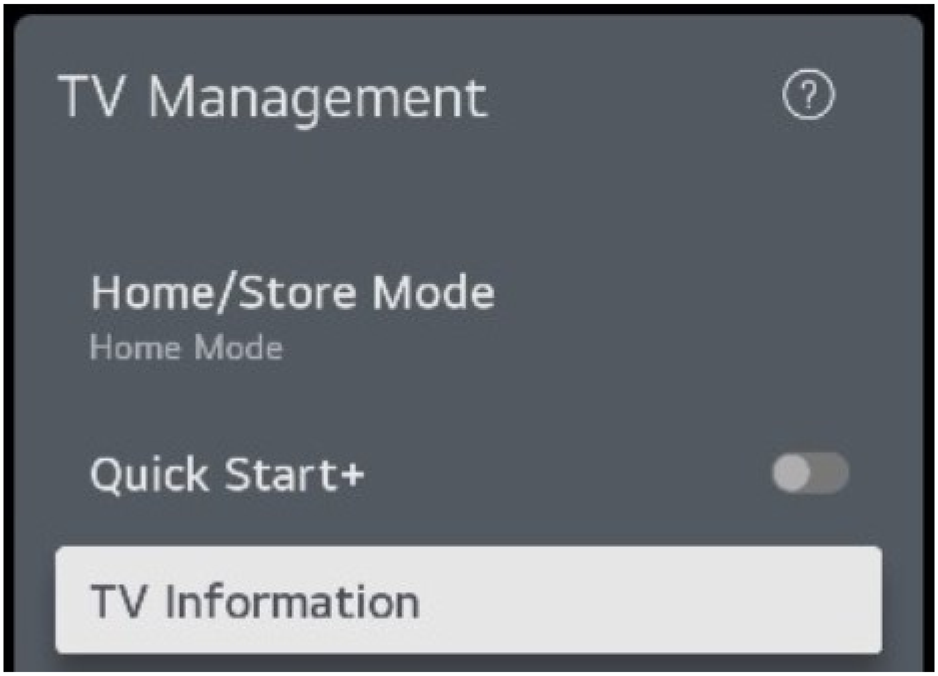


(1) Please check the p
(2) Press the
(3) For external audio

Note: This screenshot is from webOS 6. The icons and some menu items are different on webOS 7.

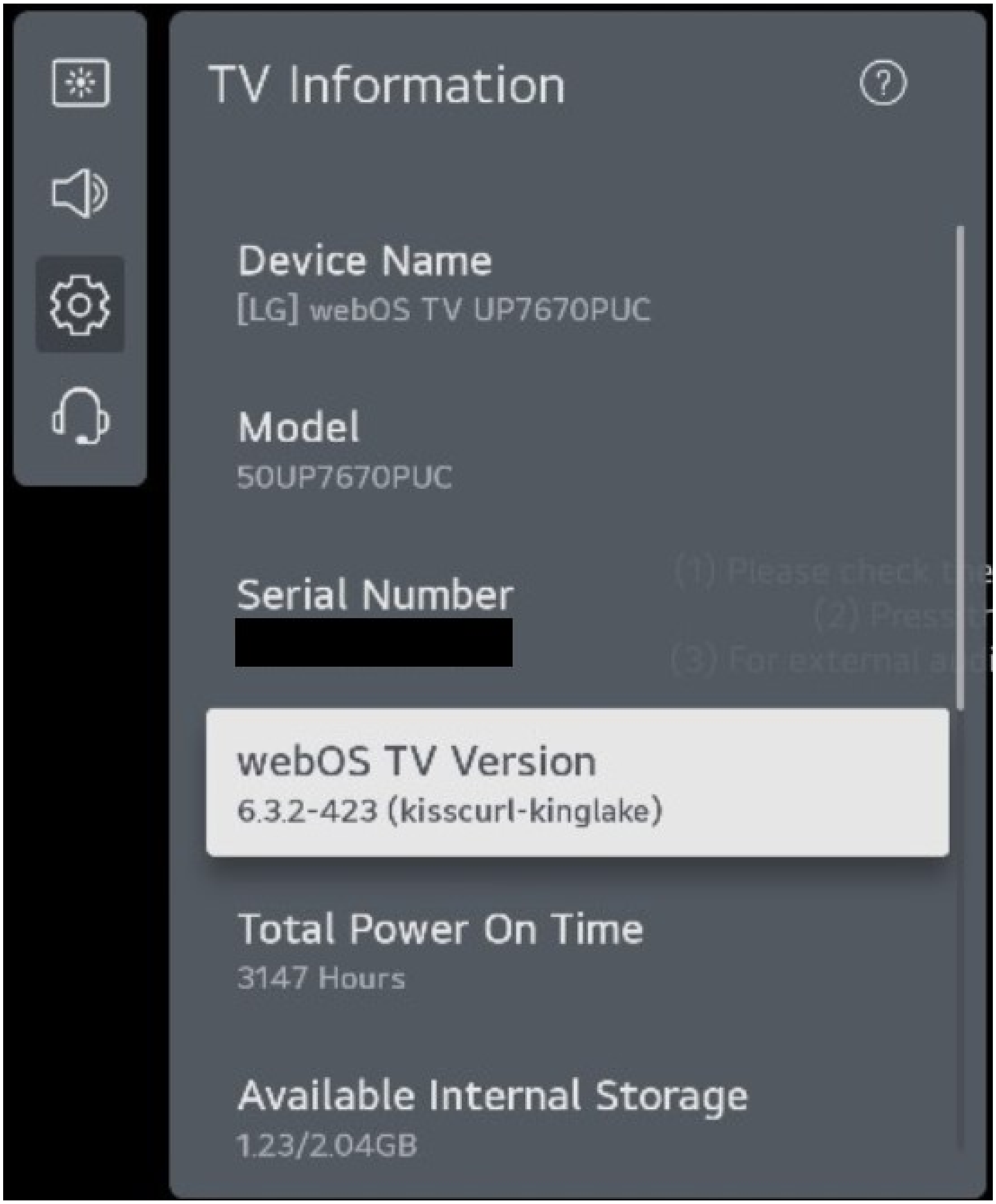
Then select "TV Management", followed by "TV Information":





Home/Store Mode
Home Mode

The webOS version is under "webOS TV Version":



TV Information

Device Name
[LG] webOS TV UP7670PUC

Model
50UP7670PUC

Serial Number
[redacted]

webOS TV Version
6.3.2-423 (kisscurl-kinglake)

Total Power On Time
3147 Hours

Available Internal Storage
1.23/2.04GB

How can I find my TV's IP address?

The TV may have up to two IP addresses: one for the wired connection, and one for Wi-Fi. You can find the IP address for each interface by in the settings menu under "Network".

You can check whether you have the right IP address for your TV by connecting to either `http://<tv ip>:3000/` or `https://<tv ip>:3001/` in a web browser. At least one of these ports should be open as long as you have screen share/second screen/"LG Connect" enabled. Port 3000 should show a `Hello world` message, while you will likely get a certificate error on port 3001 (and bypassing that should also result in `Hello world`).

How do I reboot the TV?

If your TV is already rooted, you can use the "System reboot" feature on the Homebrew Channel settings screen or run the `reboot` command via SSH or telnet. These are effective regardless of whether Quick Start+ is enabled.

If Quick Start+ is not enabled, turning the TV off (so that the red standby LED comes on) and back on is usually sufficient. However, OLED TVs will sometimes appear to be off when they are actually running the Pixel Refresher. The Pixel Refresher is triggered on shutdown when the TV has been on for more than four hours since its previous run. To make sure that an OLED (or any TV) is actually off, you can unplug it. Unplugging the TV will also force a fresh boot when Quick Start+ is enabled.

If you *still* have trouble getting a proper reboot (possibly due to Snapshot Boot), you should be able to force a reboot by disabling certain EULA options. You can then re-enable them after the reboot.

Rooting

Why do I get a `No such file or directory` error?

LG released a new developer mode jail configuration around 2023-01-26 that does not mount `/var/log/crashd` . It results in an error like this:

```
~ $ touch /var/log/crashd/"x;telnetd -l sh"
touch: /var/log/crashd/x;telnetd -l sh: No such file or directory
```

This configuration is downloaded by the Developer Mode app. It is located in `/media/developer` and named `jail_app.conf` . It is accompanied by `jail_app.conf.sig` , a cryptographic signature used to prevent a modified configuration from working. However, if `jail_app.conf` is not present a default configuration will be used. Since the default configuration does mount `/var/log/crashd` , it will work for our purposes.

Deleting `/media/developer/jail_app.conf` and rebooting the TV would allow the exploit to work until an update to the Developer Mode app in March 2023. The permissions of `/media/developer` were restricted so that `jail_app.conf` could no longer be deleted. Its contents could still be overwritten with the same result, but firmware updates rolled out starting in June of 2023 prevent a jailed application from running when `jail_app.conf` exists without a valid signature. Therefore, an old version of `jail_app.conf` is now required.

Why didn't I see any output after running a command?

Some commands, such as `touch`, do not produce output when successful. As long as you do not see an error message, it likely worked. Dev Manager displays a blue `>` when the last command succeeded and a red one when it failed.

Why am I unable to connect to telnet with PuTTY?

Make sure your PuTTY configuration is correct:

- Under "Connection type", select "Other" and "Telnet"
- "Port" should be 23 (the default when "Telnet" is selected)
- Ensure you are using the correct IP address for your TV

You can check whether the exploit was successful by running `pgrep telnetd` in the Dev Manager terminal. If the telnet server is running, this command will output a number. (The number itself is the process ID of the telnet server and is not important.)

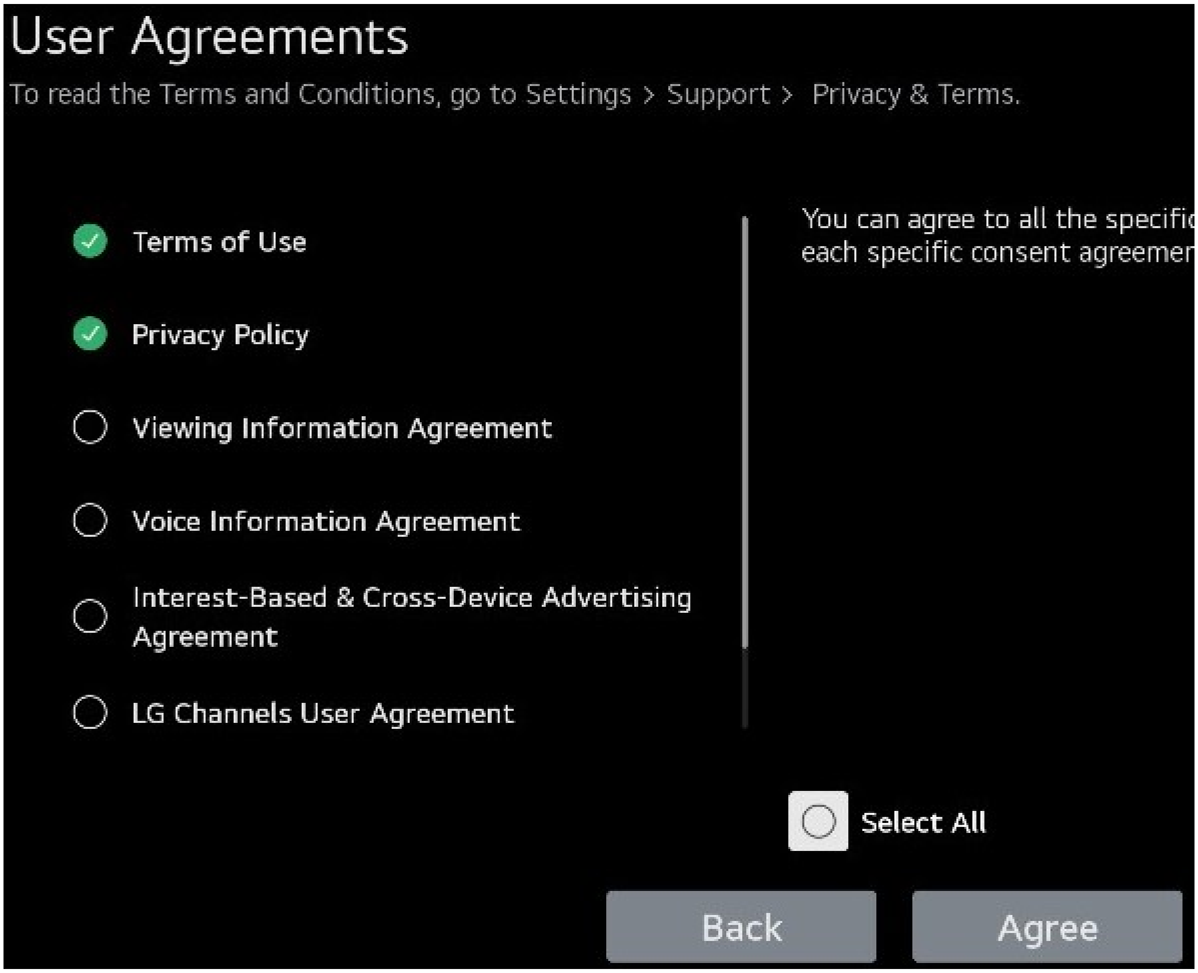
Why am I seeing `LD_PRELOAD` errors while rooting?

These errors appear because LG set an environment variable incorrectly. They are harmless, but you can prevent them from appearing by running this command:

```
unset LD_PRELOAD
```

Why isn't `telnetd` starting?

Certain EULAs must be accepted in order for this exploit to work. If the `touch` command is successful but `telnetd` does not start, this may be the problem. There are two primary EULAs ("Terms of Use" and "Privacy Policy") that are known to be needed, at least in the United States. Other regions may require additional EULAs and/or have a single UI option control multiple underlying EULA settings. You can use the command below to check what you're actually enabling.



User Agreements

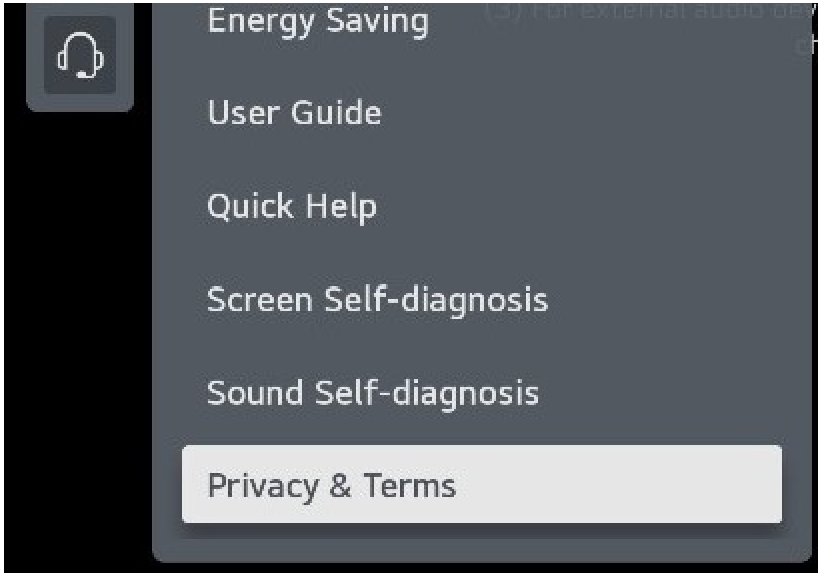
To read the Terms and Conditions, go to Settings > Support > Privacy & Terms.

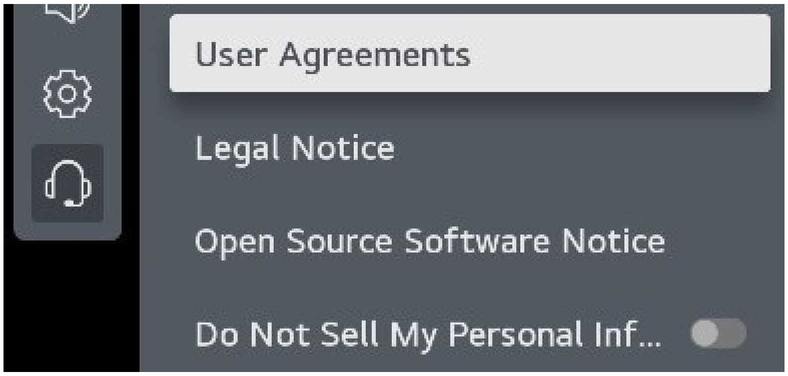
- ✓ Terms of Use
- ✓ Privacy Policy
- ○ Viewing Information Agreement
- ○ Voice Information Agreement
- ○ Interest-Based & Cross-Device Advertising Agreement
- ○ LG Channels User Agreement

You can agree to all the specifi
each specific consent agreemen

Two EULAs accepted on webOS 6.

Changing "Privacy Policy" via the UI requires a reboot. How to find the EULA screen depends on the webOS version. On webOS 6, it can be reached by pressing the menu button then choosing All Settings > Support > Privacy & Terms > User Agreements.





This command will tell you which EULAs have been accepted:

```
luna-send-pub -f -n 1 'luna://com.webos.settingsservice/getSystemSettings'
'{"keys":["eulaStatus"]}'
```

The "Terms of Use" and "Privacy Policy" agreements correspond to `networkAllowed` and `generalTermsAllowed` , respectively.

How do I download the key for the developer mode SSH server?

To download the private key, named `webos_rsa` , "Key Server" must be enabled in the Developer Mode app. You don't need to reboot after enabling it. When it's enabled, the key file will be available via HTTP on port 9991. Thus it can be downloaded with a web browser at `http://<TV IP>:9991/webos_rsa` .

The `webos_rsa` file is encrypted. The passphrase needed to decrypt it is the 6-character string shown in the LG Developer Mode app.

Can I use something other than Dev Manager?

The webOS CLI tools can run commands and install apps on webOS TVs. You can find some additional information about using these on the webosbrew site. Note that there are some differences between the webOS OSE CLI tools and the webOS TV ones.

Any decent SSH client can also be used to run commands on the TV. The OpenSSH `ssh` client is commonly available on Linux and is an optional feature on recent versions of Windows. Assuming you've downloaded the private key file from the TV and have it in the current directory, you can SSH to the TV with the following command:

```
ssh -i webos_rsa -p 9922 prisoner@<TV IP>
```

The passphrase for the key is the 6-character string displayed in the LG Developer Mode app. It is case-sensitive. If you get an error like `PTY allocation request failed on channel 0`, you won't have a prompt or some shell features, but you should still have sufficient functionality to run commands and see their output.

Note that you may need additional options to allow older SSH features depending on your client. For example, you may get an error like this:

```
Unable to negotiate with 192.168.1.123 port 9922: no matching host key type
found. Their offer: ssh-rsa
```

You should be able to solve the problem by adding the options `-oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa` to the `ssh` command above.

If you want to use PuTTY, you'll have to convert the key file to PuTTY's PPK format using PuTTYgen. Open PuTTYgen and import the key using "Import key" in the "Conversions" menu. You'll need the 6-character passphrase displayed in the LG Developer Mode app to decrypt it. After it's loaded, you can optionally change or remove the passphrase for the generated PPK by editing the "Key passphrase" and "Confirm passphrase" fields. (If you leave them alone, the PPK will have the same passphrase as the original key.) To save the PPK file, click the "Save private key" button.

Apps can be installed by transferring the IPK using SFTP then running `luna-send-pub` on the TV with the appropriate arguments. To connect with the OpenSSH command-line `sftp` client, you can use:

```
sftp -i webos_rsa -P 9922 prisoner@<TV IP>
```

How do I install an app from the command line?

App installation is triggered over the Luna bus. The `prisoner` user available in developer mode has limited access to the Luna bus using the `luna-send-pub` command. To install an app, the IPK file must already be on the TV. Files can be transferred using SFTP.

The Luna endpoint for installing developer mode apps is `luna://com.webos.appInstallService/dev/install` . Luna calls include a JSON payload. For this endpoint, the `id` , `ipkUrl` , and `subscribe` parameters are required. The path of the IPK is supplied in `ipkUrl` . Setting `subscribe` to `true` (along with the `-i` flag) means that multiple response messages will be sent as the status of the request changes. The contents of `id` are not important here.

For example, if the IPK of the app you want to install exists at `/tmp/app.ipk` , you could use the following command to install it:

```
luna-send-pub -i 'luna://com.webos.appInstallService/dev/install'
'{"id":"com.ares.defaultName","ipkUrl":"/tmp/app.ipk","subscribe":true}'
```

There will be a series of messages as the installation progresses. After the process completes, you'll have to press control+C to kill `luna-send-pub` .

Note that developer mode apps are installed in a different location than apps installed via the store, and they are deleted when developer mode is disabled or expires.

Why doesn't the Dev Mode app's key server stay enabled after rebooting?

That's how it's supposed to work. The key server is only necessary the first time you connect to the TV. Dev Manager downloads the key file and saves it for future use. (For other clients, you usually have to download the key file yourself.) You may need to enable the key server again if you do something that changes the key (e.g., factory reset) or you are connecting from a different client that doesn't already have the key. Otherwise, the same key will continue to work.

How can I verify the signature of `jail_app.conf`?

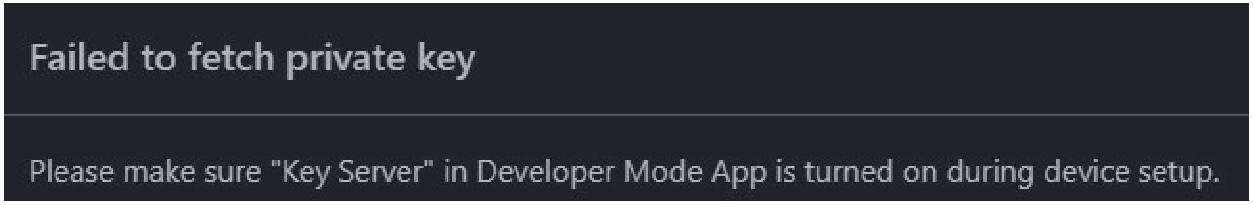
If you would like to verify that your `jail_app.conf` and `jail_app.conf.sig` match, you can use the following command:

```
openssl smime -verify -noverify -inform pem -in jail_app.conf.sig -content
jail_app.conf >/dev/null
```

Why can't I add my TV in Dev Manager?

When you add a device in using the "Developer Mode" authentication method, Dev Manager downloads the RSA key from an HTTP server on port 9991. This is what "Key Server" in the Developer Mode app refers to.

If you get a "failed to fetch private key" error when trying to add your TV in Dev Manager, Dev Manager was unable to retrieve the RSA key.



Failed to fetch private key

Please make sure "Key Server" in Developer Mode App is turned on during device setup.

Make sure you are using the correct IP address for your TV. You can try downloading the key with a web browser to check that the Key Server is working.

If you're unable to download the key, the problem is likely on the TV side. You can try disabling and re-enabling Dev Mode to fix the key server. If it still doesn't work, try leaving Developer Mode enabled and forcing a reboot using the EULA method. Remember to re-enable the Key Server after rebooting.

After rooting

Why do I still see update notifications?

Homebrew Channel's startup scripts currently run relatively late in the boot process. This means the TV's update program has already started by the time Homebrew Channel's "Block system updates" option has had a chance to take effect. If you want to make sure updates are completely disabled (and not see the notifications), block these domains (e.g., on your router):

```
snu.lge.com
su.lge.com
su-ssl.lge.com
snu-ssl.lge.com
snu-dev.lge.com
su-dev.lge.com
nsu.lge.com
```

(Listed roughly in order of importance.)

Why doesn't SSH (or telnet/other services) start at boot?

Note that the autostart method used by Homebrew Channel 0.5.1+ on webOS 4.5+ only works when certain EULAs have been accepted. Which EULAs are required depends on your region but seem to be the same as those discussed in this section.

webOS 4.0–4.4

The method used for autostart by Homebrew Channel 0.5.1+ only works on webOS 4.5+. A new autostart method will be implemented in future Homebrew Channel versions, but you can try setting it up manually yourself. It is described here. You can also try the webosbrew-autostart app as a workaround.

webOS 4.5–4.9

There is a bug in Homebrew Channel 0.5.1 that may prevent the `startup.sh` file from being automatically installed on webOS versions older than 5.0. This was fixed in Homebrew Channel 0.6.0. You can also install the startup script manually:

```
mkdir -p /var/lib/webosbrew
cp /media/developer/apps/usr/palm/services/org.webosbrew.hbchannel.service/startu
chmod 755 /var/lib/webosbrew/startup.sh
chown root:root /var/lib/webosbrew/startup.sh
```

webOS 7/22

If you are using Homebrew Channel 0.5.1 on webOS 22 (internally, webOS 7), the included SSH server won't work. Homebrew Channel 0.6.0 and later include binaries that are compatible with webOS 22. If for some reason you can't update Homebrew Channel, patched binaries are attached to previous revisions of this guide.

Should I re-enable Quick Start+ after rooting?

It's up to you. Just be aware that when Quick Start+ is on, turning the TV off won't actually shut it down. If you need to perform a proper reboot (e.g., so that startup scripts will run), you can use "System reboot" on the Homebrew Channel settings page.

Can I update to a new firmware release?

In general, updating is not recommended because LG could fix vulnerabilities used for rooting. As of this writing (2023-12-28), the `crashd` vulnerability ***will be patched soon***, although you *may* retain root during a firmware update with Homebrew Channel 0.5.1+. (Note that this does not necessarily apply if your TV was rooted with RootMyTV or GetMeIn.)

You should be aware that the most recent firmware for webOS 4.5+ now requires a valid `jail_app.conf`, which may not have been the case when you originally followed this guide. The guide has been updated to reflect this.

If you are going to ask about anything relating to a specific firmware version, **please provide an OTAID** so people can know what you're talking about.

How do I find my TV's OTAID?

The OTAID is an identifier included in every EPK (i.e., firmware image) and used with LG's SNU update system to request the latest firmware update information. There are several ways to find your TV's OTAID.

First, you can use `nyx-cmd` (this may not work if you don't have root):

```
nyx-cmd DeviceInfo query hardware_id
```

Second, it should be in `/var/run/nyx/device_info.json`, which contains JSON-formatted output from `nyx-cmd`. You can view it by running `cat /var/run/nyx/device_info.json`, and the OTAID will be on the `hardware_id` line. This file also has other information such as the TV's model number and SoC. You may not want to share its full contents in public, as it contains unique identifiers for your TV (specifically: the serial number, MAC address(es), and NDUID).

Third, you can use a Luna request, which should not require root:

```
luna-send-pub -n 1 'luna://com.webos.service.tv.systemproperty/getSystemInfo'
'{"keys":["otaId"]}'
```

The `otaId` key seems to only be available on webOS 4.0+. Use another method for earlier webOS versions (but note that webOS versions prior to 4.0 are **not vulnerable** to the `crashd` exploit).

Another option is to make a request over SSAP to the URI `ssap://com.webos.service.update/getCurrentSWInformation` with an empty payload (`{}`). The response's `model_name` property will contain the OTAID.

How do I perform a firmware downgrade?

LG has blocked firmware downgrades, even with "expert mode" enabled. Downgrades are only allowed when an AccessUSB device is connected. (AccessUSB devices are hardware tokens that enable debug access. They are presumably provided to LG partners on a limited basis.)

Can I update to a new webOS version?

While updating your firmware may increase the webOS minor version, it is usually not possible to update across major versions. This includes updating from 3.4 to 3.5+ or 4.4 to 4.5+.

However, in late 2023 LG announced their webOS Re:New program (with an apparent internal codename of `pine`), which will eventually allow certain high-end 2022 models to be upgraded to webOS 8 (a.k.a. webOS 23). So far (2024-01-12) this is not officially available outside of Korea, and changing your NSU Mode in order to upgrade early may get you into trouble unless you really know what you're doing. The only SoCs that LG currently seems to be working on support for are O22 (including O228K) and K8Hp.

How do I install APKs on webOS?

You can't. APKs are for Android, and webOS is not Android.

Can I redirect audio output through a USB DAC?

While it may be possible to build the appropriate kernel drivers, it is unlikely you would be able to get much of the TV's audio output to use such a device. Some audio goes through PulseAudio (and ALSA output is directed through PulseAudio), but the media playback pipeline uses proprietary, undocumented SoC audio peripherals. It may (or may not) be theoretically possible to reverse engineer these enough to be able to redirect audio, but it would almost certainly be a major undertaking requiring significant skill and a substantial time commitment.

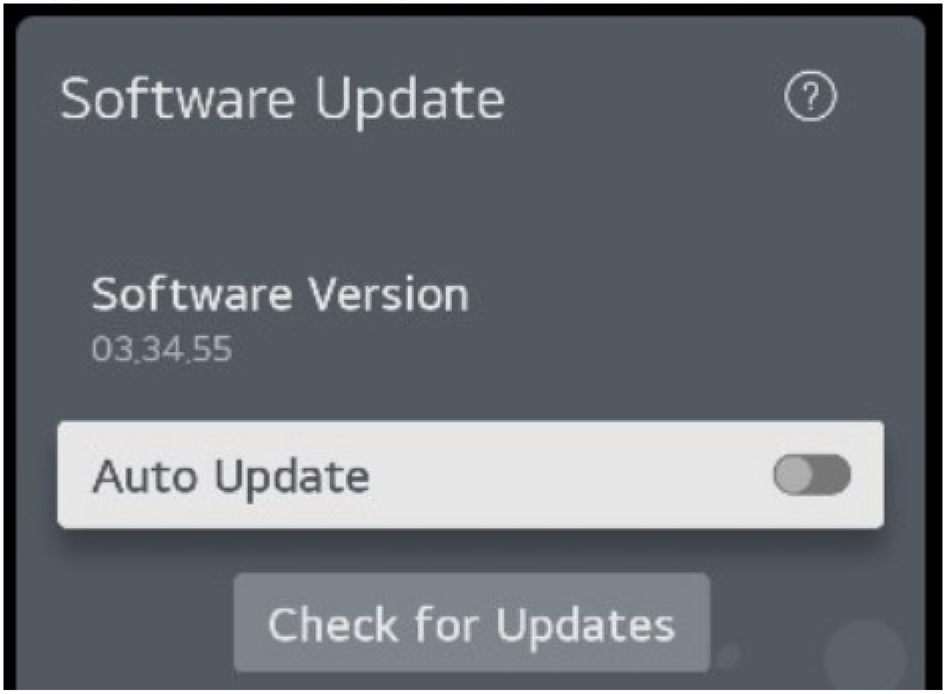
Can I add support for new filesystems?

You can build the kernel modules needed to support various filesystems. However, you would not be able to truly integrate any of them into webOS, as filesystem support is hardcoded in various system applications such as Attached Storage Manager (ASM) and Physical Device Manager (PDM).

How do I disable automatic firmware updates?

The "Auto Update" setting can be found in the menu. The steps to reach this setting vary across webOS versions.

On webOS 6, it can be found by pressing the menu button, choosing "All Settings", "Support", then "Software Update":



Software Update

Software Version
03.34.55

Auto Update

The firmware version is also displayed here.

Why are all my apps deleted after 6 weeks (or after rebooting)?

If all your installed apps are being deleted 6 weeks or so after installation (due to the expiration of the development mode timer, which is now 1000 hours) or on boot, your TV is likely not properly rooted. The `/var/luna/preferences/devmode_enabled` directory created during the above procedure should stop development mode apps from being deleted.

You should not install the LG developer mode app when rooted, as it can cause all apps to be removed. The existence of `/var/luna/preferences/devmode_enabled` as a directory may prevent LG's developer mode app from working. If you lose root access while this directory exists, a factory reset may be required in order to get the developer mode app working.

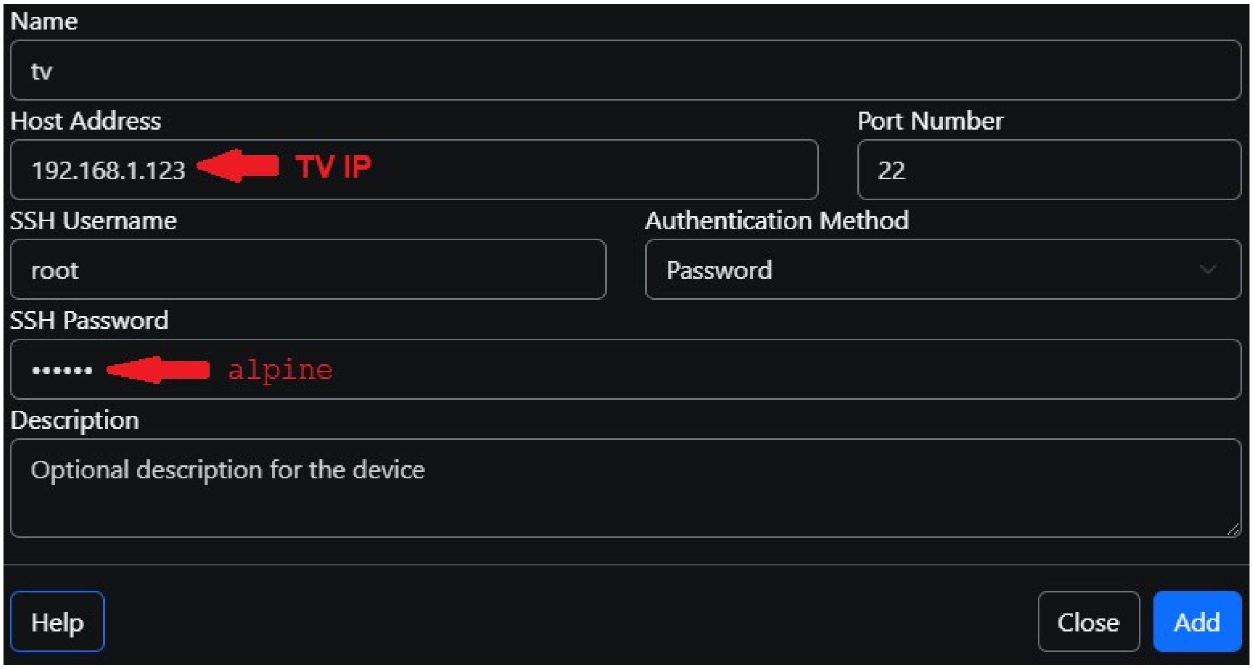
Why did I lose root after updating the Homebrew Channel app?

LG changed something in webOS 7 that causes Homebrew Channel's self-update feature to fail in all versions prior to 0.6.3. **If you have webOS 22/7, don't update Homebrew Channel from within the app** unless it's at least version 0.6.3. Updating Homebrew Channel using current versions of Dev Manager (at least through v1.9.11) will also cause root to be lost.

You can use the Homebrew Channel Updater tool, which is in the default Homebrew Channel repo, to safely update on webOS 7. It is also possible to update manually as long as you keep a telnet/SSH session open to run `/media/developer/apps/usr/palm/services/org.webosbrew.hbchannel.service/elevate-service` after the update completes and before rebooting.

Why can't I connect to my TV with Dev Manager after uninstalling the LG Developer Mode app?

The SSH server on port 9922 is provided by LG's Developer Mode app, which is uninstalled at the end of the rooting process. After rooting, you can enable Homebrew Channel's SSH server, which uses port 22. You'll need to reconfigure Dev Manager to use this new SSH server, including changing the login credentials. The easiest way to accomplish this is adding a new device within Dev Manager.

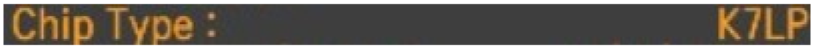

Name: tv
Host Address: 192.168.1.123
Port Number: 22
SSH Username: root
Authentication Method: Password
SSH Password: ••••••
Description: Optional description for the device

How to configure Dev Manager to connect to a TV using the default password.

The username is `root`. If you have not set up public key authentication, you must select "Password" from the "Authentication Method" dropdown and enter the password `alpine`. If you are using a public key, you'll need to choose the "Local Private Key" authentication method, then enter its name and passphrase. The key file itself must be placed in the `~/.ssh` directory (or `%USERPROFILE%\.ssh` on Windows). Note that current versions of Dev Manager support a somewhat limited range of key types.

How do I determine what SoC my TV has?

The name of the SoC is displayed in the Instart menu next to "Chip Type".


Chip Type : K7LP

This TV has a Realtek K7Lp SoC.

You can also find it by running this command:

```
nyx-cmd DeviceInfo query device_name
```

The same information can be found in the file `/var/run/nyx/device_info.json`, which is created at boot from the output of `nyx-cmd`.

Can I install Android (or some other OS) on my LG TV?

The practical answer is no. LG uses a secure boot system that verifies the signatures of all system components. The TV will refuse to boot if anything (e.g., bootloader, kernel, root filesystem) is not signed with the correct LG key. Additionally, there is no documentation or code available for most of the interesting peripherals (such as the video pipeline), meaning a hypothetical Android system would not be particularly useful.

While it is technically possible to bypass some of the secure boot chain and run unsigned code, all existing attempts to do so are proofs of concept and nowhere near ready for any kind of serious use.

How can I free up space on my TV?

The eMMC storage on many webOS TVs is not very large. The filesystem structure is also complex, with many partitions being mounted in multiple places. The vast majority of usable space is on either the `apps` or `data` partition. The mount points of the `apps` partition (which, as its name suggests, primarily stores apps) include `/media` and `/mnt/lg/appstore` . Most of the other writable space (including `/home` , `/var` , and several directories under `/mnt/lg/cache`) is on the `data` partition, which is mounted at `/mnt/lg/cmn_data` .

You can use `findmnt` and `df` to get more information about mount points and free space. The names and sizes of all eMMC partitions are listed in `/proc/partinfo` . Some models ship with large sample files in `/media/preload/storedemo` that do not seem to be important.

As an example, on a 2018 TV with an LM18A SoC, the `apps` partition has a total size of less than 600 MB, while the `data` partition is exactly 500 MiB. This TV had a 300 MB+ video named `/media/preload/storedemo/Swiss_171026_LCD_UHD_HDR_01.lge` ; deleting it has not caused any problems.

License

Donations

I have a large collection of TV boards and supporting hardware that I use for development and testing of stuff like this. It can get expensive (especially with all the weird cables LG likes to use). If you can afford to, please donate via ko-fi to support my work. I also may be interested in TV parts (and other electronics or test/measurement gear).

Load earlier comments...

l4v4l4mp3 commented on Nov 24, 2023 • edited ▾

So is 0.33.90 still safe to upgrade to. The comment above mine is indicating that at least.

//Working fine

FetchFast commented on Nov 24, 2023

I see no reason to upgrade?

raphaeleduardo42 commented on Nov 25, 2023

Worked flawless on 50ur871c0sa!
I had to manually power off from the socket in order to work those reboot actions, but no other issue faced.
I took it out of the box and did the process.

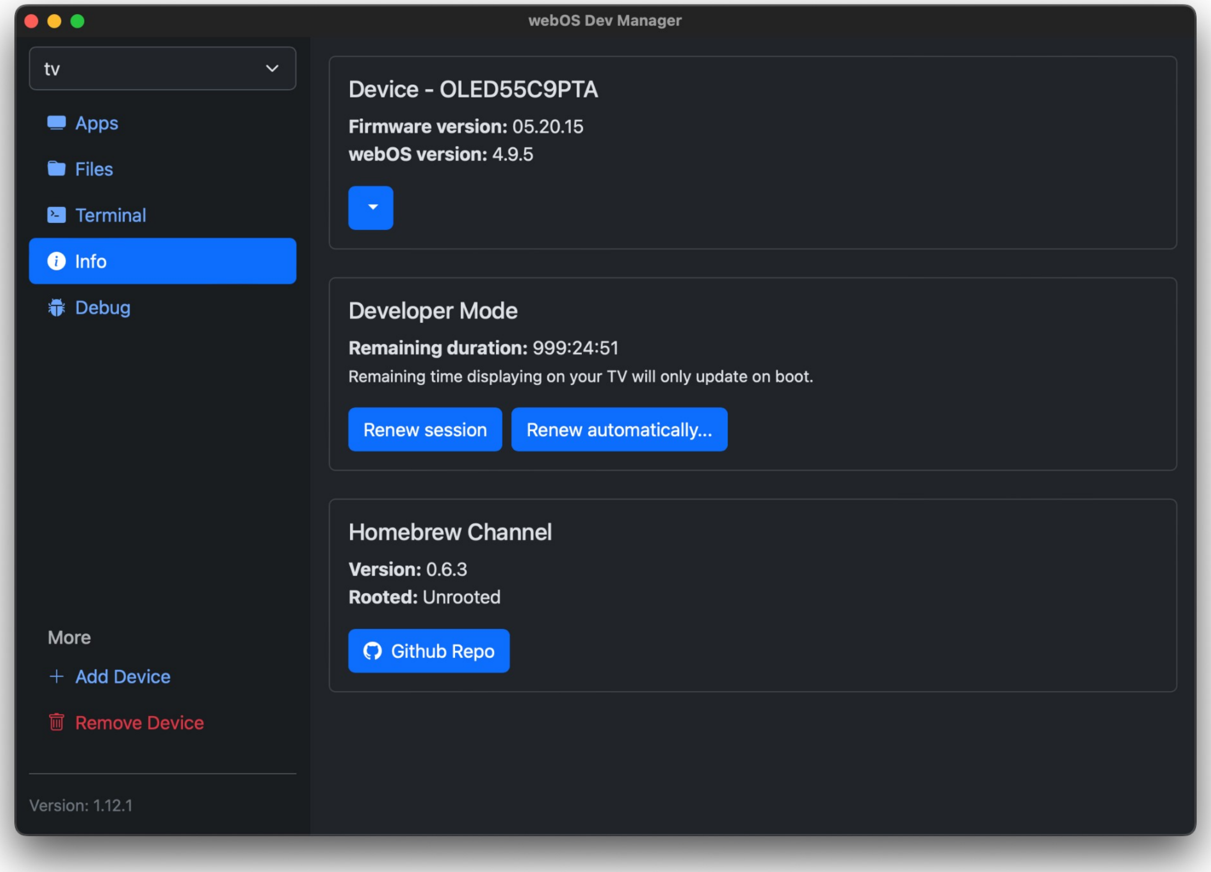
throwaway96 commented on Nov 26, 2023 Author

@leejuan126

1. Is SSH enabled in the Homebrew Channel settings? You can also try connecting using a different SSH client.
2. See this answer.

maxexcloo commented on Nov 30, 2023 • edited ▾

I'm able to follow all the steps to step 8 and am getting no output when running the command. However telnetd isn't running and I have a crash in webOS Dev Manager:



Device - OLED55C9PTA

Firmware version: 05.20.15
webOS version: 4.9.5

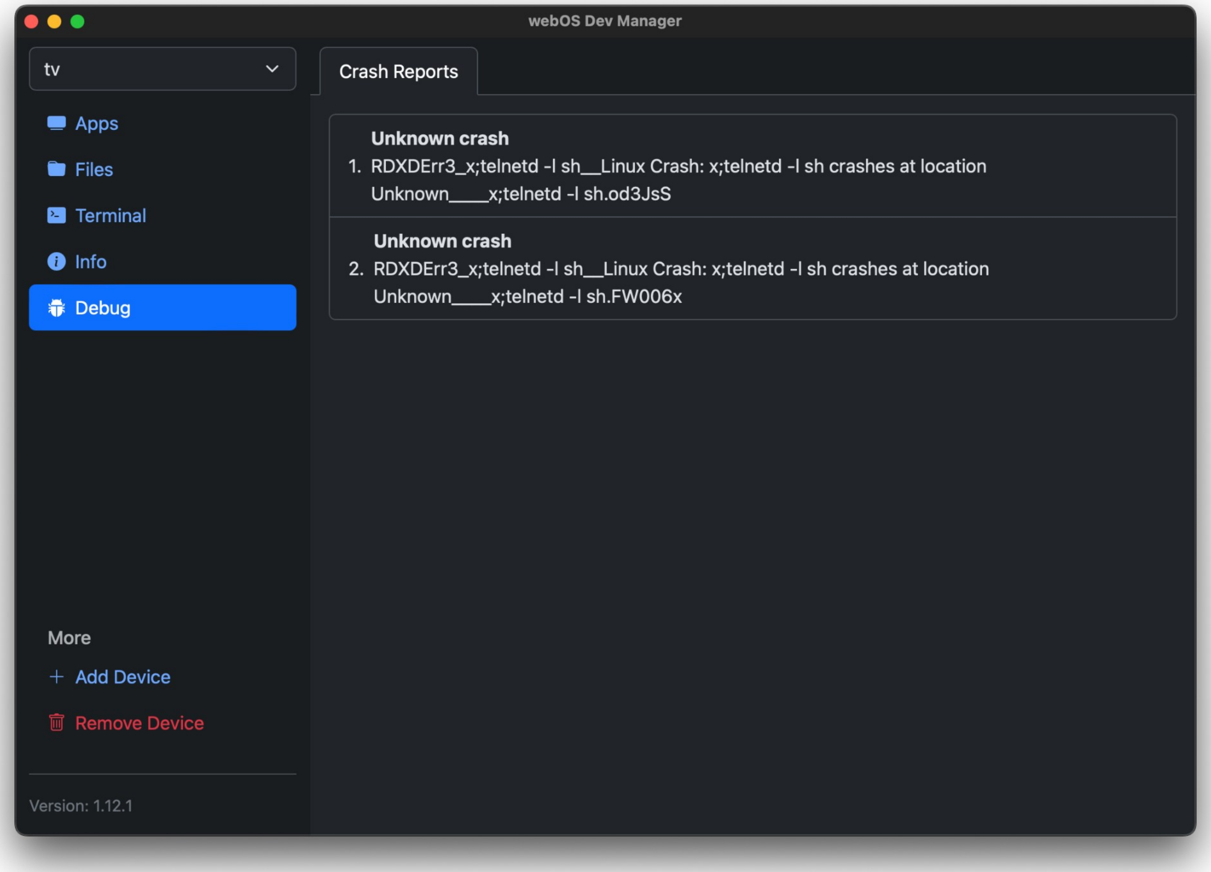
Developer Mode

Remaining duration: 999:24:51
Remaining time displaying on your TV will only update on boot.

Homebrew Channel

Version: 0.6.3
Rooted: Unrooted

Version: 1.12.1



Unknown crash
1. RDXDErr3_x;telnetd -l sh__Linux Crash: x;telnetd -l sh crashes at location Unknown____x;telnetd -l sh.od3JsS

Unknown crash
2. RDXDErr3_x;telnetd -l sh__Linux Crash: x;telnetd -l sh crashes at location Unknown____x;telnetd -l sh.FW006x

```
{ "returnValue": true, "otaId": "HE_DTV_W19O_AFABABAA" }
```

```
  {
      "subscribed": false,
      "method": "getSystemSettings",
      "settings": {
          "eulaStatus": {
              "additional3Allowed": false,
              "additionalDataAllowed": false,
              "takeOnAllowed": false,
              "additional2Allowed": false,
              "additional1Allowed": false,
              "networkAllowed": true,
              "generalTermsAllowed": true,
              "chpAllowed": false,
              "customAdAllowed": false,
              "remoteDiagAllowed": false,
              "acrOnAllowed": false,
              "thirdPartySharingAllowed": false,
              "cookiesAllowed": false,
              "customadsAllowed": false,
              "additional5Allowed": false,
              "acrAllowed": false,
              "voice2Allowed": false,
              "voiceAllowed": false,
              "additional4Allowed": false,
              "acrGdprAllowed": false,
              "acrAdAllowed": false
          }
      },
      "returnValue": true
  }
```

I haven't updated for a while so not sure what's up here...

EDIT: Alright! Enabling all the TOS items fixed it, rooted and then disabled 👯

throwaway96 commented on Nov 30, 2023 • edited ▾ Author

Having the crash reports show up but `telnetd` not launch seems to be a common symptom of not having the right EULAs accepted.

For anyone else that runs into this, I would like to hear which additional EULAs are required and what region you're in. There has been a suggestion in the past that "Viewing Information Agreement" was required in Canada (although I don't know which `eulaStatus` key this corresponds to).

throwaway96 commented on Dec 3, 2023 Author

@AndrewEfimov2005

Did you uninstall the Developer Mode app before rebooting?

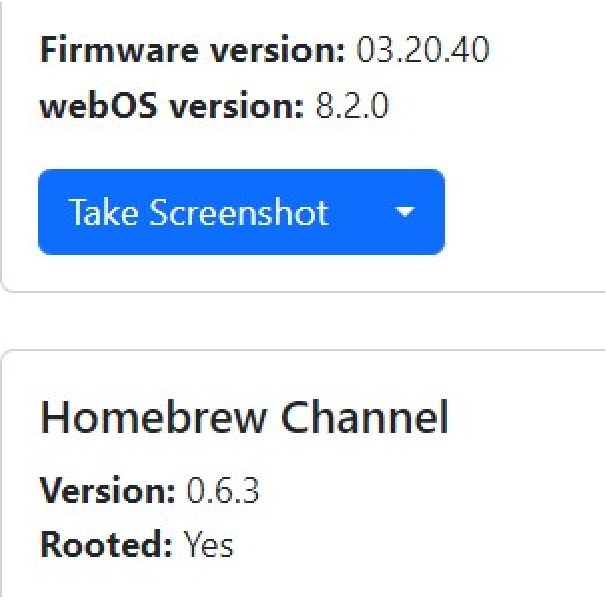
throwaway96 commented on Dec 3, 2023 Author

@AndrewEfimov2005

You need to uninstall the Developer Mode app in step 10.

marcussacana commented on Dec 4, 2023

WebOS 8.2 FW 03.20.40, crashd still works



Firmware version: 03.20.40

webOS version: 8.2.0

Homebrew Channel

Version: 0.6.3

Rooted: Yes

vsterian commented on Dec 11, 2023 • edited ▾

Hey!

I get "No such file or directory" when running touch /var/log/crashd/"x;telnetd -l sh".

I actually saw that there is a mention of this scenario on the FAQ, but I don't understand what needs to be actually done (if any). Can someone help here?

Fixed! manually navigated to var/log/crashd

leejuan126 commented on Dec 11, 2023

> @leejuan126
>
> 1. Is SSH enabled in the Homebrew Channel settings? You can also try connecting using a different SSH client.
> 2. See this answer.

Hi @throwaway96, Thanks for your reply. I had root successfully after I had re-do your introduction again.

flortsch commented on Dec 11, 2023

LG Oled G3, updated to 03.20.17, root still working.

MrToupet commented on Dec 14, 2023

> Hallo lieber Meister, ich habe ein Problem in Punkt 14. Wenn ich den SHH-Server im Homebrew Channel einschalte und den Fernseher neu starte, verschwindet das Homebrew Channel-Programm und das Konto im Entwicklermodus stürzt ab und ich muss mich dort anmelden. Ich möchte darauf hinweisen, dass dies bei allen anderen Neustarts nicht der Fall ist

@AndrewEfimov2005 Hast du eine Lösung? Habe Das selbe Problem...

psychowood commented on Dec 21, 2023 • edited

> I'm trying to install the .ipk file but it gives me an error I fail to understand: Failed to install org.webosbrew.hbchannel_0.6.3_all.ipk cannot be parsed as a URL
>
> any idea?

@Vahn84 I'm having the same issue, did you manage to solve it? Are you using macOS, by chance?

EDIT: Managed to bypass it by going in the Info tab and installing from there :)

Majkysek commented on Dec 22, 2023 • edited

is It safe to update to SW File(Version 03.40.70)? On 55OLEDB1

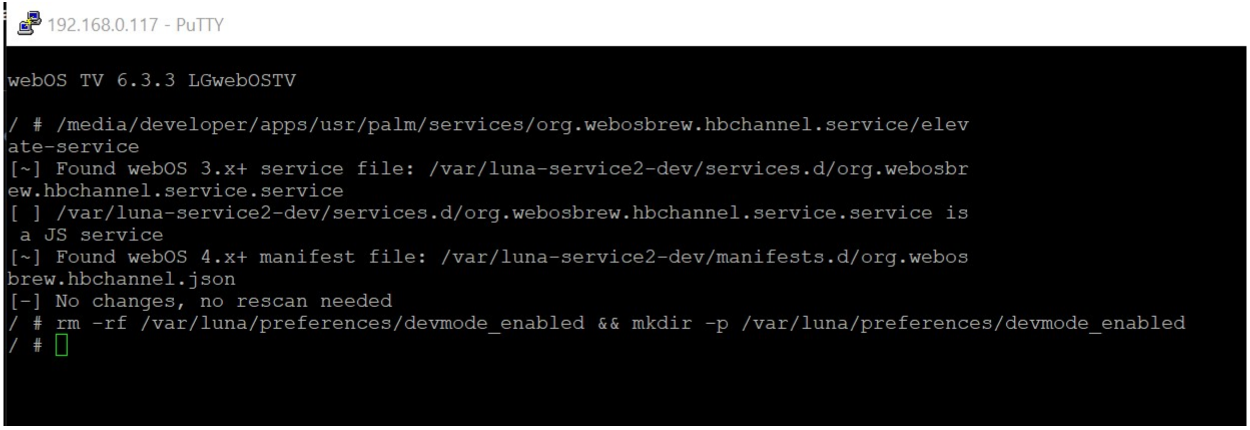
greatwitedragon commented last month

Trying to use dev mode but keep getting connected refused

stoneowx commented 3 weeks ago • edited

Hey,

Everytime I delete developer mode my apps disappear and when I looked at the Faq it said it had to do with the "***rm -rf /var/luna/preferences/devmode_enabled && mkdir -p /var/luna/preferences /devmode_enabled***" command.
But when I try to execute this command in PuttY I get no response (see screenshot).
Am I doing anything wrong?



```
webOS TV 6.3.3 LGwebOSTV

/ # /media/developer/apps/usr/palm/services/org.webosbrew.hbchannel.service/elev
ate-service
[~] Found webOS 3.x+ service file: /var/luna-service2-dev/services.d/org.webosbr
ew.hbchannel.service.service
[ ] /var/luna-service2-dev/services.d/org.webosbrew.hbchannel.service.service is
 a JS service
[~] Found webOS 4.x+ manifest file: /var/luna-service2-dev/manifests.d/org.webos
brew.hbchannel.json
[-] No changes, no rescan needed
/ # rm -rf /var/luna/preferences/devmode_enabled && mkdir -p /var/luna/preferences/devmode_enabled
/ # 
```

throwaway96 commented 3 weeks ago Author

@stoneowx

What do you mean by "Everytime I delete developer mode"? You're uninstalling it before rebooting, right?

Do you have a modified `/media/cryptofs/apps/usr/palm/services/com.palmdts.devmode.service/start-devmode.sh` ?

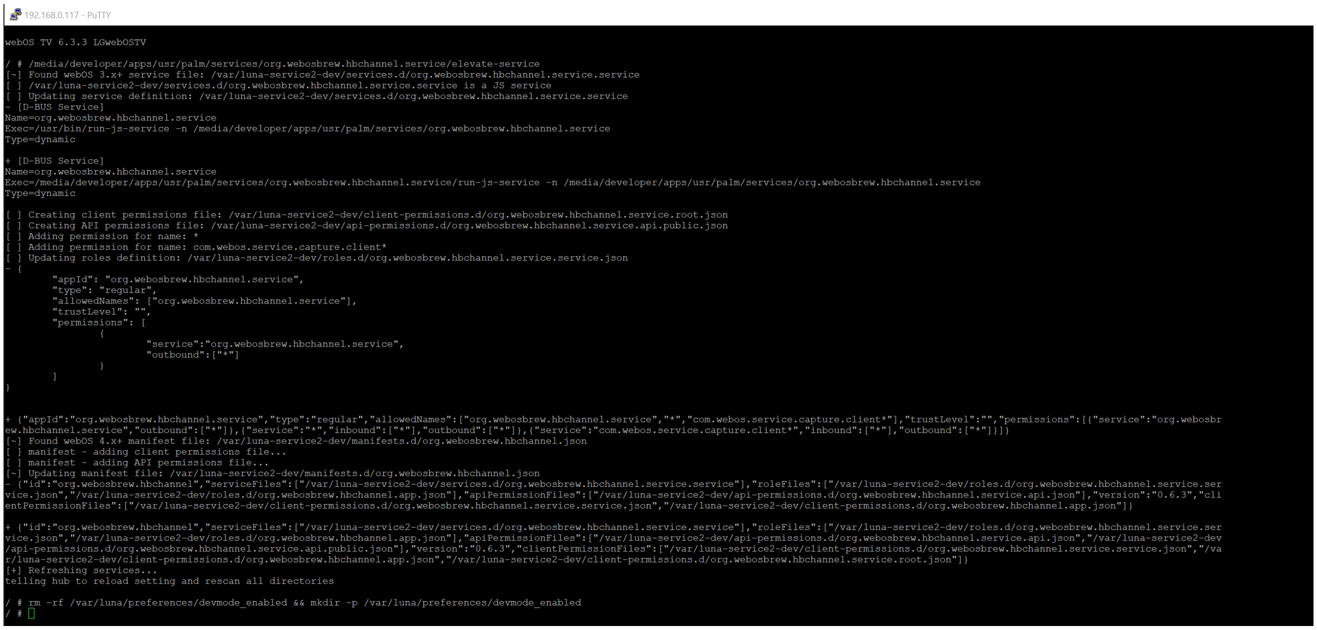
stoneowx commented 3 weeks ago

@throwaway96

I tried the whole proces over a few times from scratch, the only time I deleted developer mode is at step 10 and I didn't reboot before deleting developer mode.
Thats what I was trying to say with "Everytime I delete developer mode".

Its just whenever I would delete it the other apps will also get deleted instantly, after rebooting I'm back at step 1.

I'm using the same ***/media/cryptofs/apps/usr/palm/services/com.palmdts.devmode.service/start-devmode.sh*** as mentioned at step 9, I just redid the command to get a quick screenshot.
Here is a better one:



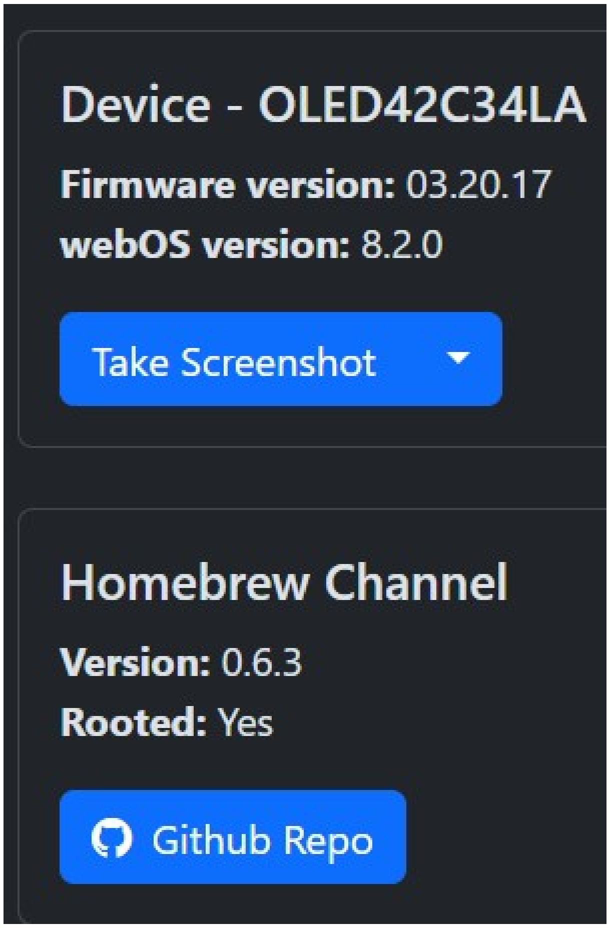
```
webOS TV 6.3.3 LGwebOSTV

/ # /media/developer/apps/usr/palm/services/org.webosbrew.hbchannel.service/elevate-service
[~] Found webOS 3.x+ service file: /var/luna-service2-dev/services.d/org.webosbrew.hbchannel.service.service
[ ] /var/luna-service2-dev/services.d/org.webosbrew.hbchannel.service.service is a JS service
[ ] Updating service definition: /var/luna-service2-dev/services.d/org.webosbrew.hbchannel.service.service
- [D-BUS Service]
Name=org.webosbrew.hbchannel.service
Exec=/usr/bin/run-js-service -n /media/developer/apps/usr/palm/services/org.webosbrew.hbchannel.service
Type=dynamic

+ [D-BUS Service]
Name=org.webosbrew.hbchannel.service
Exec=/media/developer/apps/usr/palm/services/org.webosbrew.hbchannel.service/run-js-service -n /media/developer/apps/usr/palm/services/org.webosbrew.hbchannel.service
Type=dynamic

[ ] Creating client permissions file: /var/luna-service2-dev/client-permissions.d/org.webosbrew.hbchannel.service.root.json
[ ] Creating API permissions file: /var/luna-service2-dev/api-permissions.d/org.webosbrew.hbchannel.service.api.public.json
[ ] Adding permission for name: *
[ ] Adding permission for name: com.webos.service.capture.client*
[ ] Updating roles definition: /var/luna-service2-dev/roles.d/org.webosbrew.hbchannel.service.service.json
- {
        "appId": "org.webosbrew.hbchannel.service",
        "type": "regular",
        "allowedNames": ["org.webosbrew.hbchannel.service"],
        "trustLevel": "",
        "permissions": [
                {
                        "service":"org.webosbrew.hbchannel.service",
                        "outbound":["*"]
                }
        ]
}


+ {"appId":"org.webosbrew.hbchannel.service","type":"regular","allowedNames":["org.webosbrew.hbchannel.service","*","com.webos.service.capture.client*"],"trustLevel":"","permissions":[{"service":"org.webosbr
ew.hbchannel.service","outbound":["*"]},{"service":"*","inbound":["*"],"outbound":["*"]},{"service":"com.webos.service.capture.client*","inbound":["*"],"outbound":["*"]}]}
[~] Found webOS 4.x+ manifest file: /var/luna-service2-dev/manifests.d/org.webosbrew.hbchannel.json
[ ] manifest - adding client permissions file...
[ ] manifest - adding API permissions file...
[~] Updating manifest file: /var/luna-service2-dev/manifests.d/org.webosbrew.hbchannel.json
- {"id":"org.webosbrew.hbchannel","serviceFiles":["/var/luna-service2-dev/services.d/org.webosbrew.hbchannel.service.service"],"roleFiles":["/var/luna-service2-dev/roles.d/org.webosbrew.hbchannel.service.ser
vice.json","/var/luna-service2-dev/roles.d/org.webosbrew.hbchannel.app.json"],"apiPermissionFiles":["/var/luna-service2-dev/api-permissions.d/org.webosbrew.hbchannel.service.api.json"],"version":"0.6.3","cli
entPermissionFiles":["/var/luna-service2-dev/client-permissions.d/org.webosbrew.hbchannel.service.service.json","/var/luna-service2-dev/client-permissions.d/org.webosbrew.hbchannel.app.json"]}

+ {"id":"org.webosbrew.hbchannel","serviceFiles":["/var/luna-service2-dev/services.d/org.webosbrew.hbchannel.service.service"],"roleFiles":["/var/luna-service2-dev/roles.d/org.webosbrew.hbchannel.service.ser
vice.json","/var/luna-service2-dev/roles.d/org.webosbrew.hbchannel.app.json"],"apiPermissionFiles":["/var/luna-service2-dev/api-permissions.d/org.webosbrew.hbchannel.service.api.json","/var/luna-service2-dev
/api-permissions.d/org.webosbrew.hbchannel.service.api.public.json"],"version":"0.6.3","clientPermissionFiles":["/var/luna-service2-dev/client-permissions.d/org.webosbrew.hbchannel.service.service.json","/va
r/luna-service2-dev/client-permissions.d/org.webosbrew.hbchannel.app.json","/var/luna-service2-dev/client-permissions.d/org.webosbrew.hbchannel.service.root.json"]}
[+] Refreshing services...
telling hub to reload setting and rescan all directories

/ # rm -rf /var/luna/preferences/devmode_enabled && mkdir -p /var/luna/preferences/devmode_enabled
/ # 
```

Feel free to add me on discord if that makes things easier: **stoneowx**

iGom commented 3 weeks ago

`OTAID: HE_DTV_W23O_AFABATAA`

Rooted at 03.20.14 updated to 03.20.17, root still working.



Device - OLED42C34LA

Firmware version: 03.20.17

webOS version: 8.2.0

Homebrew Channel

Version: 0.6.3

Rooted: Yes

DAT-SQUAZZ commented 3 weeks ago • edited

Thanks for the guide, I successfully rooted my OLED42C3
In webOS 8 Quick Start+ is in Settings->General->System->Additional Settings

Tequila-dev commented 3 weeks ago

Getting Timeout while contacting DNS servers while downloading jailpatch.sh. How to fix this?

Full error code:
0curl: (6) Could not resolve: raw.githubusercontent.com (Timeout while contacting DNS servers)

Tequila-dev commented 3 weeks ago

> Getting Timeout while contacting DNS servers while downloading jailpatch.sh. How to fix this?
>
> Full error code: 0curl: (6) Could not resolve: raw.githubusercontent.com (Timeout while contacting DNS servers)

Fixed by downloading and importing jailpatch.sh manually within Dev Manager files system

Majkysek commented 3 weeks ago

> is It safe to update to SW File(Version 03.40.70)? On 55OLEDB1

I will answer myself. I just updated and the tv is still rooted.

ElPumpo commented 2 weeks ago • edited

My OLED77C36LC auto updated to firmware 03.30.60 which is super weird since I have auto update disabled.

But since I was rooted prior, I keep it after updating?

webOS 8.3.0

skarakolev commented 2 weeks ago

Hi, I've completed all the steps and it says **Root status: ok**, but when I try to install an app from Homebrew Channel, I get the following error message:

```
An error occured during installation: -1 Unknown method "install" for category "/dev"
```

What am I doing wrong?

SSShuva commented 2 weeks ago

Question: TV OLED 65C1 is it possible to get root on firmware 03.36.50?
Can I upgrade to this firmware before getting root?

popy2k14 commented 2 weeks ago

> > is It safe to update to SW File(Version 03.40.70)? On 55OLEDB1
>
> I will answer myself. I just updated and the tv is still rooted.

Thx for the hint. Will update my 65OLEDB1 tv.

djvdberg commented last week • edited

> Hey!
>
> I get "No such file or directory" when running touch /var/log/crashd/"x;telnetd -l sh".
>
> I actually saw that there is a mention of this scenario on the FAQ, but I don't understand what needs to be actually done (if any). Can someone help here?
>
> Fixed! manually navigated to var/log/crashd

How, please help? **@vsterian**

precupstefan commented 11 hours ago

Thank you very much! I confirm it is working on 03.20.50