CVITEK Cyber Security Precautions for SDK Secondary Development

Version： 2.0.0

Release date: 2023-02-08

CONTENTS

Revision History

Revision	Date	Description
1.0.0	2022/06/10	Initial
2.0.0	2023/02/08	Compatible with cv180x/cv181x

CHAPTER

ONE

DISCLAIMER

Terms and Conditions

The document and all information contained herein remain the CVITEK Co., Ltd' s ("CVITEK") confidential information, and should not disclose to any third party or use it in any way without CVITEK' s prior written consent.

User shall be liable for any damage and loss caused by unauthority use and disclosure.

CVITEK reserves the right to make changes to information contained in this document at any time and without notice.

All information contained herein is provided in "AS IS" basis, without warranties of any kind, expressed or implied, including without limitation mercantability, non-infringement and fitness for a particular purpose.

In no event shall CVITEK be liable for any third party' s software provided herein, User shall only seek remedy against such third party.

CVITEK especially claims that CVITEK shall have no liable for CVITEK' s work result based on Customer' s specification or published shandard.

Contact Us

Address Building 1, Yard 9, FengHao East Road, Haidian District, Beijing, 100094, China

Building T10, UpperCoast Park, Huizhanwan, Zhancheng Community, Fuhai Street, Baoan District, Shenzhen, 518100, China

Phone +86-10-57590723 +86-10-57590724

Website https://www.sophgo.com/

Forum https://developer.sophgo.com/forum/index.html

CHAPTER

TWO

OVERVIEW

The products based on CVITEK chip solutions may face the related network security threats. The main purpose of this document is to provide the corresponding solutions to these problems from the perspective of network security.

CHAPTER

THREE

CVITEK CYBER SECURITY PRECAUTIONS FOR SDK SECONDARY DEVELOPMENT

3.1 Precautions for using u-boot

3.1.1 Serial Port

The u-boot serial port function in CVITEK SDK is enabled by default. In the execution process of u-boot, u-boot will wait for one second, so that the developers can interrupt the execution process of u-boot by hitting the key in the execution phase, so as to stay in the u-boot phase for debugging. If there is no keystroke in the process, the boot process of u-boot will continue after one second.

In the officially released product, you can cancel this configuration in order to achieve the purpose of not to debug through serial port at u-boot stage. The specific implementation method is as follows:

Step 1. Open build/boards/{chip_name}/{board_name}/u-boot{board_name}_defconfig (there may be different file names depending on the name of each product, in this example it is cvitek_cv1801c_wevb_0009a_spinor_defconfig)。Modify the configuration value of "CONFIG_BOOTDELAY" to "-2" .

```
...
CONFIG_IDENT_STRING=" cvitek_cv180x"
CONFIG_DISTRO_DEFAULTS=y
CONFIG_BOOTDELAY=-2
# CONFIG_DISPLAY_CPUINFO is not set
...
```

Step 2. Recompile u-boot

3.1.2 U-boot Commands

U-boot provides many commands for developers to develop and debug, such as md, mw, setenv, saveenv, etc. However, these commands are not necessary in official products. You can choose to keep the commands that are not related to system security and delete other commands.

For example, to delete the md/mw commands, the specific implementation is as follows:

Open /u-boot-2021.10/cmd/Makefile, Since the specific implementation code of md/mw is in mem.c, directly comment out or delete obj-$(CONFIG_CMD_MEMORY) += mem.o in the example below.

```
obj-$(CONFIG_LOGBUFFER) += log.o
obj-$(CONFIG_ID_EEPROM) += mac.o
obj-$(CONFIG_CMD_MD5SUM) += md5sum.o
#obj-$(CONFIG_CMD_MEMORY) += mem.o
obj-$(CONFIG_CMD_IO) += io.o
obj-$(CONFIG_CMD_MFSL) += mfsl.o
```

Or revise /u-boot-2021.10/cmd/Kconfig, and configure default to "n".

```
config CMD_MEMORY
        bool "md, mm, nm, mw, cp, cmp, base, loop, ip_update"
        default n
        help
         Memory commands.
            md - memory display
            mm - memory modify (auto-incrementing address)
            nm - memory modify (constant address)
            mw - memory write (fill)
            cp - memory copy
            cmp - memory compare
            base - print or set address offset
            loop - initialize loop on address range
            ip_update - sync ip from mem 0x400038C/900 to uboot env
```

Other commands deletion methods are similar to the above operations.

3.2 Security precautions when using networks in Linux

3.2.1 Root Account

In actual products, it is necessary to make security modifications to the root user. Users can choose to change the default password or disable root login via shell. The specific methods are as follows:

- Change the password

  Step 1. Execute the shell command "passwd" to change the password

  Step 2. Copy /etc/shadow (through mount SD card or network)

  Step 3. Copy the shadow file to /ramdisk/rootfs/overlay/{chip_name}/etc

  Step 4. Recompile the rootfs file system (Command: `pack_rootfs`), and burn rootfs.spinor back to the platform

- Disable root login via shell

  Step 1. Modify /ramdisk/rootfs/overlay/{chip_name}/etc/passwd in the SDK package and change the script

  `root:x:0:0:root:/root:/bin/sh`

  to:

  `root:x:0:0:root:/root:/bin/false`

  Step 2. Recompile rootfs file system (command: `pack_rootfs`), and burn the rootfs.spinor back to the platform.

3.2.2 File Permissions

CVITEK SDK uses SquashFS file system by default. Users are unable to perform write or delete actions on the pre-loaded file system, thereby protecting the stability of the system.

3.3 Security precautions when using network drivers in Linux

3.3.1 Serial Port

Developers can debug through the serial port in Linux. In order to avoid the risk of illegal access to the serial port and make sure that the serial port is no longer used in the product, they can close the serial port in mass production state. The specific implementation method is as follows:

Step 1. Open build/boards/{chip_name}/{board_name}/dts /{chip_name}/{chip_name}_base.dtsi (There may be different file names depending on the product names, in this example: cv180x), modify the code of the following example,

```
  uart0: serial@04140000 {
              compatible = "snps,dw-apb-uart";
              reg = <0x0 0x04140000 0x0 0x1000>;
              clock-frequency = <25000000>;
              reg-shift = <2>;
              reg-io-width = <4>;
-             status = "okay";
+             status = "disabled";
     };
```

Step 2. Recompile linux

3.4 Safety Notifications for Application Development

3.4.1 Cipher Driver

CIPHER is a security algorithm module provided by CVITEK media processing platform. It provides symmetric encryption and decryption algorithms, including AES / DES / SM4, asymmetric encryption and decryption algorithm, RSA random number generation, and digest algorithm, including HASH and HMAC. Customers can use it to encrypt and decrypt audio and video streams, and to authenticate the legitimacy of users.

Please refer to 《CVITEK CIPHER API Reference》 for details.

3.5 Other Safety Notifications

3.5.1 Bare Burning

CVITEK SDK package provides SD and USB bare burning function. It is recommended to turn off the bare burning function in actual products. SD, USB bare burning function can be turned off through hardware design.

3.5.2 SD Card/USB Mount Permission

If the developed product has SD card or USB and other pluggable storage device interfaces, it is recommended to add the "- o noexec" parameter before mounting the file system of the storage device, so as to avoid the damage of the system caused by the operation of malicious third-party programs.

3.5.3 JTAG

It is suggested that JTAG interface should be removed from actual products to avoid system damage caused by malicious tampering with system configuration.