Home Releases Submit Vuln Press About PGP Contact Tutorials Supporters Projects

Sick.Codes

HOME RELEASES SUBMIT VULN PRESS ABOUT PGP CONTACT TUTORIALS SUPPORTERS PROJECTS

Home › Security

CVE-2020-27402 – Hindotech HK1 TV Box – Root Privilege Escalation

by Sick Codes – October 12, 2020 - Updated on November 24, 2020 in Security, Tutorials 0

SICK-2020-004 Hindotech HK1 TV Box - Root Privilege Escalation - Improper Access Control

CVE-2020-27402

Hindotech HK1 TV Box – Root Privilege Escalation – Improper Access Control

CVE ID

CVE-2020-27402

CVSS Score

7.8

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Internal ID

SICK-2020-004
SICK-2020-005

Vendor

- Hindotech, Shenzhen Hindo Technology Co.,Ltd

- Hindotech, Hong Kong Hindo Technology Co.,Ltd

Product

HK1 Box S905X3 TV Box

Product Version

HK1_X3_S905X3_4BIT_V11_2019-11-05

Vulnerability Details

The HK1 Box S905X3 TV Box contains a vulnerability that allows a local unprivileged user, such as a malicious APK, to escalate to root using the /system/xbin/su binary. While connected to the device through the serial port (UART), or while using adb as an unprivileged user, the local attacker can execute the /system/xbin/su binary and execute arbitrary code as root, steal social networking account tokens, WiFi passwords, cookies, saved passwords, user location data, message history, emails, or contacts, etc.

A local attacker using adb, or a physical attacker connecting to the device through the UART serial debugging port, is dropped into a shell as the “shell” user without entering a username or password.

Once logged in as the “shell” user, the attacker can escalate to root using the /sbin/su binary which is group executable (750), or /system/xbin/su which is executable by all users (755).

In order to use the device in its intended way, victims are encouraged to sign-in to all of their favorite TV, email, music, and social networking related apps & accounts.

An attacker can steal any social networking account cookies or session tokens, read saved passwords, reveal user location data, emails, message history, contacts, or use the HK1 Box maliciously to sniff other devices on the same network, usually in a home networking environment.

For example, once root, the network WiFi password can be read in plain text at /data/misc/wifi/WifiConfigStore.xml.

Vendor Response

None

Disclosure Timeline

* **2020-09-20** - Vulnerability identified & researcher prepares report
* **2020-09-21** - Researcher unable to reach (502 error) manufacturers website hindotech.com
* **2020-09-22** - Researcher submits draft advisory to Amlogic instead (No response, not the vendor.)
* **2020-10-09** - Researcher still unable to reach (502 error) manufacturers website.
* **2020-10-09** - Researcher submits draft advisory to Shenzhen Hindo Technology Co.,Ltd. email
* **2020-10-12** - Researcher still unable to reach (502 error) manufacturers website.
* **2020-10-12** - Researcher receives no response from anyone and publishes research.
* **2020-11-03** - CVE assigned CVE-2020-27402

Credits

@sickcodes - https://twitter.com/sickcodes/

Links

https://sick.codes/sick-2020-004/

https://github.com/sickcodes/security/blob/master/advisories/SICK-2020-004.md

https://twitter.com/sickcodes

http://hindotech.com/

https://github.com/sickcodes

https://sick.codes/

Exploit Proof of Concept

Connect via adb or using the UART serial port:

```
whoami
# shell

/system/xbin/su
whoami
# root
```

```
grep PreSharedKey /data/misc/wifi/WifiConfigStore.xml
# <string name="PreSharedKey">&quot;WIFIPASSWORD&quot;</string>
```

Mitigation

Protect your HK1 Box

Connect via adb or using the UART serial port:

```
whoami
# shell

/system/xbin/su
whoami
# root

chmod 700 /system/xbin/su
chmod 700 /sbin/su
```

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Website

Privacy - Terms

I am human

POST COMMENT

@sickcodes

@sickcodes

@sickcodes

Discord Server

sickcodes.slack.com

t.me/sickcodeschat

./contact_form