#### Title

Local Privilege Escalation in HP Thin Pro OS

# Affected software:

- T6X44017 ftp://ftp.hp.com/pub/tcdebian/images/T6X44017.dd.gz
- T6X51007 ftp://ftp.hp.com/pub/tcdebian/images/T6X51007.dd.gz
- T6X52011 ftp://ftp.hp.com/pub/tcdebian/images/T6X52011.dd.gz
- Z6X52011 ftp://ftp.hp.com/pub/tcdebian/images/Z6X52011.dd.gz

# Credits:

- Roberto Suggi Liverani @malerisch
- Vincent Hutsebaut @vhutsebaut

# Description/Impact

In HP Thin Pro OS, the sudo configuration allows an unauthenticated user to abuse the keyboard layout tool to perform a privilege escalation attack and gain unauthorised root access on the machine.

The keyboard layout (located in "/usr/bin/hptc-keyboard-layout") runs as a privileged process and it is directly available to an unauthenticated user from the UI (user interface) of the HP Thin Pro Kiosk.

By abusing the available UI controls, an unauthenticated user can navigate on the file system and restore the original /etc/shadow file on the system, which will then allow to set a new admin password on the system.

# Conditions

The following conditions are required:

- HP Thin OS Pro set in Kiosk mode;
- HP Thin OS Pro administrator password has already been set by an administrator;

- A malicious user has physical access to the Kiosk but does not have a user account and does not know the admin password.

# Steps to reproduce (as a malicious user)

1) Click on the left side, "Control Panel" icon and then clicking the "Keyboard Layout" icon; \*\* note that the button and UI might be different from the OS version, but the keyboard layout tool is available to an unauthenticated user in Kiosk mode





2) Click on print icon, a "Print File" dialog prompt is provided to the user

Step 2 – Figure 1

Layout	<b>x</b>
Keyboard Layout	Ŋ
Primary Secondary	
Standard Keyboard: 💻 United States [English] 🗸	
Details for United States [English]	h
Model Generic 104-key PC	
Layout English (US)	
Variant Windows-Compatible	
	ב
The Keyboard Preview	
🔹 🔽 Sample Text Area	
Minimize Local Keyboard Shortcuts Ok Cancel	

Print File dialog allows to set an "output file" - by clicking on the "..." button to choose the folder
 Step 3 – Figure 1

1	🖺 Keyboard Layout 🗖 🗖 🗖			
	Keyboard Layout	(IP)		
	Primary Secondary			
or ys	Standard Keyboard: Details for United Model Generic 104 Layout English (US) Variant Windows-Co Output file: /home/user/print.pdf			
	The Keyboard Preview Options >> Print Cancel Concel			
	Sample Text Area  Minimize Local Keyboard Shortcuts Ok	Cancel		

Step 3 – Figure 2



# 4) Navigate to /etc/ folder

Step 4 – Figure 1

2	Ke	eyboard Layout		
🧟 Keyboa	ard Layout			li.
<b>1</b>	F	Print To File		
P Look in:	👼 /etc		• • •	* 🐔 🗄 🗉
Compute user S	r issue issue.net kernel-img.conf krb5.conf ld.so.cache ld.so.conf legal libccid_Info.plist locale.alias locale.gen locale.nopurge localtime login.defs lsb-base-logging.sh lsb-release magic magic.mime	mailcap mailcap.order mime.types mke2fs.conf modules mozpluggerrc mtab mtools.conf networks nsswitch.conf omnikey.ini os-release pam.conf papersize passwd passwd- printcap	profile profile.bak protocols rc.local resolv.conf rmt rpc securetty sensors3.conf services shadow shadow- shells sudoers sudoers.dpkg-dist synergy.conf	syslog.conf systeminfo timezone ucf.conf urandom.state wgetrc xdmcp.hosts xinetd.conf
File name:	print.pdf			📕 <u>S</u> ave
Files of type:	All Files (*)			▼ X Cancel

# 5) Rename /etc/shadow into /etc/shadow-last-modified-by-admin

Step 5 – Figure 1



Step 6 – Figure 1



# 6) Rename /etc/shadow- into /etc/shadow

Step 6 – Figure 1



7) Click on the "Administrator/User Mode Switch"

Step 7 – Figure 1



8) Malicious user can set a new admin password and access the administrator mode of the kiosk

Step 8 – Figure 1



# 9) Launch an xterminal with root access

Step 9 – Figure 1



Step 9 – Figure 2



# **Further observations**

The /etc/shadow- file remains as the original one even after that the admin password has been changed multiple times. In this example, passwd has already been set twice but the shadow- remains the one set originally in the OS (back in 2013), making the attack described in this report possible:

root@HP000c29a7d34d: /writable/home/user 🔤 🖬 🕱
root@HP000c29a7d34d:/writable/home/user# stat /etc/shadow
File: `/etc/shadow'
Size: 914 Blocks: 2 IO Block: 1024 regular file
Device: 11h/1/d Inode: 565 Links: 1
Hccess: (0640/-rwr) Uld: ( 0/ root) Gld: ( 42/ shadow)
Hodess: 2016-04-28 06:14:33.000000000 -0400
Change 2016-04-28 06:14:33:000000000 -0400
Birth: -
root@HP000c29a7d34d:/writable/home/user# stat /etc/shadow-
File: `/etc/shadow-'
Size: 851 Blocks: 2 IO Block: 1024 regular file
Device: 11h/17d Inode: 602 Links: 1
Access: (0600/-rw) Uid: ( 0/ root) Gid: ( 0/ root)
HCCess: 2013-10-25 12:34:43.00000000 -0400
Depres 2013-10-25 12:34:45,00000000 -0400
Births -
root0HP000c29a7d34d:/writable/home/user#_date
Thu Apr 28 06:15:33 EDT 2016
root@HP000c29a7d34d:/writable/home/user#

In the sudoer configuration, it is possible to see the NOPASSWD tag set for the Keyboard Layout tool (usr/bin/hptc-keyboard-layout):

root@HP000c29a7d34d: /writable/home/u		
# Cmnd alias specification		
# User privilege specification root ALL=(ALL) ALL		
%root ALL = NOPASSWD: ALL		
# needed by hptc-sysinfo user ALL = NOPASSWD: /usr/sbin/dmidecode		
user ALL = NOPASSWD: /sbin/reboot user ALL = NOPASSWD: /sbin/halt user ALL = NOPASSWD: /use/bin/avdm		
user ALL = NORASSWD: /bin/hpprint_app		
user HLL = NUPHSSWU: /usr/bin/hptc-touchscreen user ALL = NOPASSWD: /usr/bin/hptcktop-icon		
user ALL = NOPASSWD: /usr/bin/hptc-keyboard-layout user ALL = NOPASSWD: /usr/bin/idesk		
user ALL = NOPASSWD: /usr/bin/killall		
user ALL = NOPASSWD: /usr/bin/hptc-logger user ALL = NOPASSWD: /usr/bin/load t410 codec.sh		
user ALL = NOPASSWD: /usr/bin/hptc-system-id		
user ALL = NUPASSWD: /usr/bin/trigger_shutdown user ALL = NOPASSWD: /usr/bin/hptc-zero-status		