Hash Suite - Windows password security audit tool. GUI, reports in PDF.

Date: Tue, 6 Jul 2021 10:53:55 +0300
From: Mustafa Kuscu <mustafakuscu@...il.com>
To: oss-security@...ts.openwall.com
Subject: xscreensaver 5.45 crash

Hi,

As the embargo period has ended, I am sharing some details about an xscreensaver crash that might happen on some setups. There are i) the original post and ii) reproduction instructions.

My workaround is to stop using xscreensaver on my system. And also I have disabled TB3 port, instead, using USB-C port only, with the dock.

*i) original posting to distros: *

Hi,
This is a new issue which results in xscreensaver crash. Previously I have reported a similar issue to the Qubes OS security team. This one might be affecting other distros therefore posting to this list.

I have a Lenovo Thinkpad T14 Genl Intel laptop and a Lenovo TB3 dock with vendor firmware 1.19. My T14 laptop has 2 usb-c ports. Previously I owned a T480s which had the same two ports, and one was for power and the other was for thunderbolt.

It looks like T14 has changed the behavior of the power port. T480s could not recognize external screens through the power port, but T14 can. I might be wrong, this is just an observation. So when docking and undocking, sometimes I use the power port, sometimes the TB3 port.

The behavior in CVE-2021-34557 started after I upgraded the firmware to v1.19. The Qubes OS security team has released a patched version of xscreensaver that mitigated the crash, however, it looks like there is a new variant.

When connected to my 3 monitor setup (two external displays through the tb3 dock + laptop display), just unplug thunderbolt cable, plug it into the other port. And repeat vice versa. Within 1-2 attempts, the screensaver crashes with desktop unlocked. (These reproduction steps do not always result in a crash. Will work on it to determine how to reproduce it precisely.)

The stack trace of crashed processes are below. I am not an X11 expert, and not sure if these are related to each other. Both binaries are from the latest r4.1 branch of Qubes OS.

I also thought about notifying Lenovo but don't know of an effective means to ask for their help on the UEFI update.

Jun 20 22:24:23 dom0 systemd-coredump[50218]: Process 50175 (xrandr) of user 1000 dumped core.

Stack trace of thread 50175:
#0 0x00005efc87cf7c23 main (xrandr + 0x3c23)
#1 0x00007f77df8ce082 __libc_start_main (libc.so.6 + 0x27082)
#2 0x00005efc87cfd32e _start (xrandr + 0x932e)
Jun 20 22:24:23 dom0 systemd[1]: systemd-coredump@...0217-0.service: Succeeded.

Jun 20 21:59:10 dom0 systemd-coredump[49098]: Process 7710 (xscreensaver) of user 1000 dumped core.

Stack trace of thread 7710:
#0 0x00007725eea98bab kill (libc.so.6 + 0x3cbab)
#1 0x00007725eea98860 __restore_rt (libc.so.6 + 0x3c860)
#2 0x000063323b529ccc auth_finished_cb (xscreensaver + 0x24ccc)
#3 0x000063323b52a61f unlock_p (xscreensaver + 0x2561f)
#4 0x000063323b5115b6 main (xscreensaver + 0xc5b6)
#5 0x00007725eea83082 __libc_start_main (libc.so.6 + 0x27082)
#6 0x000063323b5122de _start (xscreensaver + 0xd2de)
Jun 20 21:59:10 dom0 systemd[1]: systemd-coredump@...9097-0.service: Succeeded.

ii) reproduction instructions
Actually I cannot review the code at the moment therefore I don't know if they are related or not.
However the new issue is reproducible. The steps to reproduce are:

shut down the laptop and dock
connect the dock to the TB3 port
boot the system
log in (3 displays)
lock the screen
plug TB3 cable off
plug it into the USB-C port
screen is unlocked

The unit systemd-coredump@...285-0.service has successfully entered the 'dead' state.
Jun 22 14:39:22 dom0 systemd-coredump[9286]: Process 8893 (xscreensaver) of user 1000 dumped core.

Stack trace of thread 8893:
#0 0x00007a8b14778bab kill (libc.so.6 + 0x3cbab)
#1 0x00007a8b14778860 __restore_rt (libc.so.6 + 0x3c860)
#2 0x00005ea8124ea69d update_passwd_window (xscreensaver + 0x2169d)
#3 0x00005ea8124ed229 passwd_event_loop (xscreensaver + 0x24229)
#4 0x00005ea8124ed9cc gui_auth_conv (xscreensaver + 0x249cc)
#5 0x00005ea8124ef2c1 pam_conversation (xscreensaver + 0x262c1)
#6 0x00007a8b1494a477 pam_vprompt (libpam.so.0 + 0x9477)
#7 0x00007a8b1494a6ce pam_prompt (libpam.so.0 + 0x96ce)
#8 0x00007a8b14946d26 pam_get_authtok_internal (libpam.so.0 + 0x5d26)
#9 0x00007a8b145c4897 pam_sm_authenticate (pam_unix.so + 0x4897)
#10 0x00007a8b149452d2 _pam_dispatch (libpam.so.0 + 0x42d2)
#11 0x00007a8b14944ba4 pam_authenticate (libpam.so.0 + 0x3ba4)

```
                                                #12 0x00005ea8124ef72c
pam_try_unlock (xscreensaver + 0x2672c)
                                                #13 0x00005ea8124eec59
xss_authenticate (xscreensaver + 0x25c59)
                                                #14 0x00005ea8124ee61f
unlock_p (xscreensaver + 0x2561f)
                                                #15 0x00005ea8124d55b6 main
(xscreensaver + 0xc5b6)
                                                #16 0x00007a8b14763082
__libc_start_main (libc.so.6 + 0x27082)
                                                #17 0x00005ea8124d62de _start
(xscreensaver + 0xd2de)
-- Subject: Process 8893 (xscreensaver) dumped core
-- Defined-By: systemd
-- Support: https://lists.freedesktop.org/mailman/listinfo/systemd-devel
-- Documentation: man:core(5)
--
-- Process 8893 (xscreensaver) crashed and dumped core.
--
-- This usually indicates a programming error in the crashing program and
-- should be reported to its vendor as a bug.

Kind Regards,

Mustafa Kuscu
```

Powered by blists - more mailing lists

Please check out the Open Source Software Security Wiki, which is counterpart to this mailing list.

Confused about mailing lists and their use? Read about mailing lists on Wikipedia and check out these guidelines on proper formatting of your messages.