corna / **me_cleaner**

funny sidequest ... race condition? #64

New issue

Open **mereportertmp12432** opened this issue 2 days ago · 2 comments

mereportertmp12432 commented 2 days ago • edited

hi, i have a pansonic cf19mk6 with qm77 chipset and this is the story of how I was able to corrupt - and hopefully disable - my ME using fwupdlcl and the integrated programmer, so it may inspire future "research".

me config

Local FWUpdate: Enabled
BIOS Config Lock: Enabled
Host Read Access to ME: Disabled
Host Write Access to ME: Disabled

behaviour for fwupdlcl with me_cleaned ME.bin

https://filebin.ca/3ZorKoSiEbI2/MEREG-muchdisable.bin
C:\UpdateMeFirmware\Data801>FWUpdLcl64.exe
-oemid D6B09D64-DA23-49A9-8888-F663BE603389 -allowsv -f "MEREG-muchdisable.bin"
Intel (R) Firmware Update Utility Version: 8.1.40.1456
Copyright (C) 2007 - 2013, Intel Corporation. All rights reserved.
Communication Mode: MEI
Checking firmware parameters...
Warning: Do not exit the process or power off the machine before the firmware update process ends.
Sending the update image to FW for verification: [COMPLETE]
FW Update: [15% (Stage: 4 of 19) (-)]
Error 8741: FW Update Failed.
Error 8707: Firmware update failed due to an internal error

partially update OEM stock ME.bin

https://filebin.ca/3ZoqtxiQEx5m/ME.bin
C:\UpdateMeFirmware\Data801>FWUpdLcl.exe -oemid D6B09D64-DA23-49A9-8888-F663BE603389
-allowsv -f "ME.bin"
Intel (R) Firmware Update Utility Version: 8.1.40.1456
Copyright (C) 2007 - 2013, Intel Corporation. All rights reserved.
Communication Mode: MEI
Checking firmware parameters...
Warning: Do not exit the process or power off the machine before the firmware update process ends.
Sending the update image to FW for verification: [COMPLETE]
FW Update: [35% (Stage: 13 of 19) (-)]

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

2 participants

HIBERNATE, after being in Stage13 for 2-3 seconds ... last seen "50%" and Stage 14/19

^C Update: [0% (Stage: 0 of 19) (|)]]

RESUME, now see 0%, program hangs, so ctrl-c && hijack session with me_cleaned ME.bin

https://filebin.ca/3ZorKoSiEbI2/MEREG-muchdisable.bin
C:\UpdateMeFirmware\Data801>FWUpdLcl.exe -oemid D6B09D64-DA23-49A9-8888-F663BE603389 -allowsv -f "MEREG-muchdisable.bin"
Intel (R) Firmware Update Utility Version: 8.1.40.1456
Copyright (C) 2007 - 2013, Intel Corporation. All rights reserved.
Communication Mode: MEI
Checking firmware parameters...
Warning: Do not exit the process or power off the machine before the firmware update process ends.
Sending the update image to FW for verification: [COMPLETE]
FW Update: [35% (Stage: 13 of 19) (-)]

it directly jumps to Stage 13 35% ... cool?

FW Update: [100% (Stage: 19 of 19) (-)]
FW Update is complete and a reboot will run the new FW.

results

other oem strings @ panasonic pcinfo http://picpaste.com/diff-pcinfo.png
PRE-BOOT and other ME-Name @ meinfo http://picpaste.com/diff-meinfo.png
Recovery state and two wiped registers @ http://picpaste.com/diff-intelmetool.png
fwupdlcl -fwver shows version, but -save and -f just hang
memanuf reports some error
ctrl-p reports "FW Status Recovery Error" and then just boots
no issues so far, doesnt powercycle after 30 min or anything. seems good to me, especially the "pre-boot" thingy ... but what the heck do i know

mereportertmp12432 commented 9 hours ago • edited

any suggestions for one of those hipster vulnerability names?
i'll throw "UpDateME" and "Sleeper Hold" in the room for starters.

archfan commented 9 hours ago

> any suggestions for one of those hipster vulnerability names?
> Hodl me tight.