BMW IDCEVO :: Kernel Crash Handling with DSS & Ramdump

Checklist

- [ ] How to capture ramdump - LK Mode
    - [ ] entire-dram (directly from dram)
    - [ ] dss only (directly from dram)
    - [ ] dss only (from ufs partition)
- [ ] How to capture ramdump - Kernel mode
    - [ ] dss only (samlldump from ufs partition)
- [ ] Ramdump with IOC watchdog
- [ ] Ramdump with SOC watchdog
- [ ] Ramdump - dss memory mapping
- [ ] Ramdump - ufs partition details

- [ ] How to align ramdump extraction tool with DSS offset ?
- [ ] How to handle - Kernel crashed but no warm reset from IOC

Release	ES4
HW Variant	B2 SP25 505
.	SYS

Ramdump collection

This page will describe how to collect ramdumps and its different modes. On kernel panic/crash IOC watchdog will do the warm reset and system will get rebooted and go to ramdump mode in LK.

One of the way to test panic trigger for ramdump collection is by executing below command in SYS/Android console.

```
#echo c > /proc/sysrq-trigger
```

Entire dram (LK Mode) - capture from dram

- On Panic, IOC/SOC watchdog will do the warm reset and system will get rebooted and go to ram dump mode in LK
- Press "s" key to stop at LK prompt
- Execute command "fast" in LK prompt.

```
#fast
This is do_fastboot
fastboot_init success!!
PHY Boot mode :ROM mode start
SUP_DIG_IDCODE_LO:0x54cd
[Current] SUP_DIG_LVL_OVRD_IN:0x0055
[Modified] SUP_DIG_LVL_OVRD_IN:0x00f5
enumeration success
```

- Once enumeration is completed, Run ram dump extraction tool on host side.

```
#python eautodump.py -m dram
=================================================================
Mode: dram
Domain: all
Section:  all
Output path: ./20230817-145851_virt_from_dram
=================================================================
DRAM dump Mode
DSS Version : 0x1100000000001211
./20230817-145851_virt_from_dram/ap_0x80000000--0x9fffffff.lst...

ramdump start address is [0x80000000]
ramdump size is [0x20000000]
starting dump
================================================================
 RECEIVED:  100 %, read bytes: 0x20000000 |===================>|
================================================================

dump success

finished. total time: 14.111s
./20230817-145851_virt_from_dram/ap_0xa0000000--0xbfffffff.lst...

ramdump start address is [0xa0000000]
ramdump size is [0x20000000]
starting dump
==============================
```

DSS only (LK mode) - capture from dram

- On Panic, IOC/SOC watchdog will do the warm reset and system will get rebooted and go to ram dump mode in LK
- Press "s" key to stop at LK prompt
- Execute command "fast" in LK prompt.

```
#fast
This is do_fastboot
fastboot_init success!!
PHY Boot mode :ROM mode start
SUP_DIG_IDCODE_LO:0x54cd
[Current] SUP_DIG_LVL_OVRD_IN:0x0055
[Modified] SUP_DIG_LVL_OVRD_IN:0x00f5
enumeration success
```

- Once enumeration is completed, Run ram dump extraction tool on host side.

#**python eautodump.py -m dss**
===
Mode: dss
Domain: all
Section: all
Output path: ./20230817-111747_virt_from_dram
===
DRAM dump Mode
DSS Version : 0x1100000000001211
./20230817-111747_virt_from_dram/VM2_header_0xe0000000--0xe000ffff.lst...

ramdump start address is [0xe0000000]
ramdump size is [0x10000]
starting dump
==
 RECEIVED: 100 %, read bytes: 0x00010000 |===================>|
==

dump success

finished. total time: 0.036s
./20230817-111747_virt_from_dram/VM2_kernel_0xe0010000--0xe020ffff.lst...

```
ramdump start address is [0xe0010000]
ramdump size is [0x200000]
starting dump
==================================================================
 RECEIVED:  100 %, read bytes: 0x00200000 |====================>|
==================================================================

dump success

finished. total time: 0.087s
./20230817-111747_virt_from_dram/VM2_platform_0xe0210000--0xe060ffff.lst...

ramdump start address is [0xe0210000]
ramdump size is [0x400000]
starting dump
==================================================================
 RECEIVED:  100 %, read bytes: 0x00400000 |====================>|
==================================================================

dump success

finished. total time: 0.160s
./20230817-111747_virt_from_dram/VM2_first_0xe0610000--0xe080ffff.lst...

ramdump start address is [0xe0610000]
ramdump size is [0x200000]
starting dump
==================================================================
 RECEIVED:  100 %, read bytes: 0x00200000 |====================>|
==================================================================

dump success

finished. total time: 0.098s
./20230817-111747_virt_from_dram/VM2_kevent_0xe0810000--0xe0a0ffff.lst...

ramdump start address is [0xe0810000]
ramdump size is [0x200000]
starting dump
==================================================================
 RECEIVED:  100 %, read bytes: 0x00200000 |====================>|
==================================================================
```

DSS only (LK mode) - capture from ufs partition

- On Panic, IOC/SOC watchdog will do the warm reset and system will get rebooted and go to ram dump mode in LK
- Press "s" key to stop at LK prompt
- set dss only mode in LK

dss at LK

```
] ramdump setmode only-dss
] ramdump only-dss
```

- Run fast command in LK prompt

```
#fast
This is do_fastboot
fastboot_init success!!
PHY Boot mode :ROM mode start
SUP_DIG_IDCODE_LO:0x54cd
[Current] SUP_DIG_LVL_OVRD_IN:0x0055
[Modified] SUP_DIG_LVL_OVRD_IN:0x00f5
enumeration success
```

- Run ramdump extraction tool in storage mode in Host side.

```
#python eautodump.py -m storage
```

DSS only (Kernel mode) - capture from ufs

steps

```
root@idcevo-hv-v920:/dev/disk/by-partlabel# ls -al
total 0
drwxr-xr-x 2 root root 2020 Jan  1 12:00 .
drwxr-xr-x 7 root root  140 Jan  1 12:00 ..
lrwxrwxrwx 1 root root   10 Jan  1 12:00 a_pit -> ../../sda1
lrwxrwxrwx 1 root root   10 Jan  1 12:00 abuf -> ../../sda3
lrwxrwxrwx 1 root root   10 Jan  1 12:00 audiofw_a -> ../../sdd7
lrwxrwxrwx 1 root root   10 Jan  1 12:00 audiofw_b -> ../../sde7
lrwxrwxrwx 1 root root   10 Jan  1 12:00 b_pit -> ../../sda2
lrwxrwxrwx 1 root root   11 Jan  1 12:00 bios-dtb -> ../../sda10
lrwxrwxrwx 1 root root   11 Jan  1 12:00 bios-dtbo -> ../../sda11
lrwxrwxrwx 1 root root   10 Jan  1 12:00 bios-kernel -> ../../sda9
lrwxrwxrwx 1 root root   11 Jan  1 12:00 bios-ramdisk -> ../../sda12
lrwxrwxrwx 1 root root   11 Jan  1 12:00 boot_a -> ../../sdf11
lrwxrwxrwx 1 root root   11 Jan  1 12:00 boot_b -> ../../sdf32
lrwxrwxrwx 1 root root   10 Jan  1 12:00 bootcontrol -> ../../sda7
lrwxrwxrwx 1 root root   10 Jan  1 12:00 buffer -> ../../sda8
lrwxrwxrwx 1 root root   11 Jan  1 12:00 buffer5_a -> ../../sdf24
lrwxrwxrwx 1 root root   11 Jan  1 12:00 buffer5_b -> ../../sdf45
lrwxrwxrwx 1 root root   10 Jan  1 12:00 comm_ng_a -> ../../sdd6
lrwxrwxrwx 1 root root   10 Jan  1 12:00 comm_ng_b -> ../../sde6
lrwxrwxrwx 1 root root   11 Jan  1 12:00 cont-camadas_a -> ../../sdf22
lrwxrwxrwx 1 root root   11 Jan  1 12:00 cont-camadas_b -> ../../sdf43
lrwxrwxrwx 1 root root   11 Jan  1 12:00 cont-huapp_a -> ../../sdf21
lrwxrwxrwx 1 root root   11 Jan  1 12:00 cont-huapp_b -> ../../sdf42
lrwxrwxrwx 1 root root   11 Jan  1 12:00 cont-telematics_a -> ../../sdf23
lrwxrwxrwx 1 root root   11 Jan  1 12:00 cont-telematics_b -> ../../sdf44
lrwxrwxrwx 1 root root   11 Jan  1 12:00 cont1_a -> ../../sdf20
lrwxrwxrwx 1 root root   11 Jan  1 12:00 cont1_b -> ../../sdf41
lrwxrwxrwx 1 root root   11 Jan  1 12:00 data -> ../../sdf63
lrwxrwxrwx 1 root root   11 Jan  1 12:00 dtbo_a -> ../../sdf14
lrwxrwxrwx 1 root root   11 Jan  1 12:00 dtbo_b -> ../../sdf35
lrwxrwxrwx 1 root root   11 Jan  1 12:00 early -> ../../sda14
lrwxrwxrwx 1 root root   11 Jan  1 12:00 efs -> ../../sdf66
lrwxrwxrwx 1 root root   10 Jan  1 12:00 env -> ../../sda4
lrwxrwxrwx 1 root root   11 Jan  1 12:00 hyp_a -> ../../sdd11
lrwxrwxrwx 1 root root   11 Jan  1 12:00 hyp_b -> ../../sde11
lrwxrwxrwx 1 root root   11 Jan  1 12:00 hyp_dtb0_a -> ../../sdd12
lrwxrwxrwx 1 root root   11 Jan  1 12:00 hyp_dtb0_b -> ../../sde12
lrwxrwxrwx 1 root root   11 Jan  1 12:00 hyp_dtb1_a -> ../../sdd13
lrwxrwxrwx 1 root root   11 Jan  1 12:00 hyp_dtb1_b -> ../../sde13
lrwxrwxrwx 1 root root   11 Jan  1 12:00 hyp_dtb2_a -> ../../sdd14
lrwxrwxrwx 1 root root   11 Jan  1 12:00 hyp_dtb2_b -> ../../sde14
lrwxrwxrwx 1 root root   11 Jan  1 12:00 hyp_dtb3_a -> ../../sdd15
lrwxrwxrwx 1 root root   11 Jan  1 12:00 hyp_dtb3_b -> ../../sde15
lrwxrwxrwx 1 root root   11 Jan  1 12:00 hyp_rsv_b -> ../../sde17
lrwxrwxrwx 1 root root   11 Jan  1 12:00 hyp_rsvd1 -> ../../sdd16
lrwxrwxrwx 1 root root   11 Jan  1 12:00 hyp_rsvd2 -> ../../sdd17
lrwxrwxrwx 1 root root   11 Jan  1 12:00 init_boot_a -> ../../sdf13
lrwxrwxrwx 1 root root   11 Jan  1 12:00 init_boot_b -> ../../sdf34
lrwxrwxrwx 1 root root   10 Jan  1 12:00 keystorage_a -> ../../sdd1
lrwxrwxrwx 1 root root   10 Jan  1 12:00 keystorage_b -> ../../sde1
lrwxrwxrwx 1 root root   11 Jan  1 12:00 metadata -> ../../sdf65
lrwxrwxrwx 1 root root   11 Jan  1 12:00 misc -> ../../sdf67
lrwxrwxrwx 1 root root   11 Jan  1 12:00 node0_dtb_a -> ../../sdd19
lrwxrwxrwx 1 root root   11 Jan  1 12:00 node0_dtb_b -> ../../sde19
lrwxrwxrwx 1 root root   11 Jan  1 12:00 node0_dtbo_a -> ../../sdd22
lrwxrwxrwx 1 root root   11 Jan  1 12:00 node0_dtbo_b -> ../../sde22
lrwxrwxrwx 1 root root   11 Jan  1 12:00 node0_kernel_a -> ../../sdd18
lrwxrwxrwx 1 root root   11 Jan  1 12:00 node0_kernel_b -> ../../sde18
lrwxrwxrwx 1 root root   11 Jan  1 12:00 node0_rootfs_a -> ../../sdd21
lrwxrwxrwx 1 root root   11 Jan  1 12:00 node0_rootfs_b -> ../../sde21
lrwxrwxrwx 1 root root   11 Jan  1 12:00 node0_unused_a -> ../../sdd23
```

```
lrwxrwxrwx 1 root root   11 Jan  1 12:00 node0_unused_b -> ../../sde23
lrwxrwxrwx 1 root root   11 Jan  1 12:00 node0_vbmeta_a -> ../../sdd20
lrwxrwxrwx 1 root root   11 Jan  1 12:00 node0_vbmeta_b -> ../../sde20
lrwxrwxrwx 1 root root   11 Jan  1 12:00 persist -> ../../sdf62
lrwxrwxrwx 1 root root   11 Jan  1 12:00 pre_buf5 -> ../../sdf10
lrwxrwxrwx 1 root root   11 Jan  1 12:00 recovery_a -> ../../sdf15
lrwxrwxrwx 1 root root   11 Jan  1 12:00 recovery_b -> ../../sdf36
lrwxrwxrwx 1 root root   10 Jan  1 12:00 secure_fw_a -> ../../sdd2
lrwxrwxrwx 1 root root   10 Jan  1 12:00 secure_fw_b -> ../../sde2
lrwxrwxrwx 1 root root   10 Jan  1 12:00 secure_os_a -> ../../sdd3
lrwxrwxrwx 1 root root   10 Jan  1 12:00 secure_os_b -> ../../sde3
lrwxrwxrwx 1 root root   11 Jan  1 12:00 sfi_early_a -> ../../sdd10
lrwxrwxrwx 1 root root   11 Jan  1 12:00 sfi_early_b -> ../../sde10
lrwxrwxrwx 1 root root   10 Jan  1 12:00 sfi_pbl_a -> ../../sdd8
lrwxrwxrwx 1 root root   10 Jan  1 12:00 sfi_pbl_b -> ../../sde8
lrwxrwxrwx 1 root root   10 Jan  1 12:00 sfi_platform_a -> ../../sdd9
lrwxrwxrwx 1 root root   10 Jan  1 12:00 sfi_platform_b -> ../../sde9
lrwxrwxrwx 1 root root   11 Jan  1 12:00 smalldump -> ../../sdf68      //smalldump partition sdf68
lrwxrwxrwx 1 root root   10 Jan  1 12:00 strongbox_a -> ../../sdd5
lrwxrwxrwx 1 root root   10 Jan  1 12:00 strongbox_b -> ../../sde5
lrwxrwxrwx 1 root root   11 Jan  1 12:00 super -> ../../sdf60
lrwxrwxrwx 1 root root   11 Jan  1 12:00 superinactive -> ../../sdf61
lrwxrwxrwx 1 root root   10 Jan  1 12:00 switch -> ../../sda5
lrwxrwxrwx 1 root root   10 Jan  1 12:00 token -> ../../sda6
lrwxrwxrwx 1 root root   10 Jan  1 12:00 tzconfig_a -> ../../sdd4
lrwxrwxrwx 1 root root   10 Jan  1 12:00 tzconfig_b -> ../../sde4
lrwxrwxrwx 1 root root   11 Jan  1 12:00 unused -> ../../sda17
lrwxrwxrwx 1 root root   11 Jan  1 12:00 userdata -> ../../sdf64
lrwxrwxrwx 1 root root   11 Jan  1 12:00 varncd -> ../../sda16
lrwxrwxrwx 1 root root   11 Jan  1 12:00 varsys -> ../../sda15
lrwxrwxrwx 1 root root   11 Jan  1 12:00 vbmeta_a -> ../../sdf16
lrwxrwxrwx 1 root root   11 Jan  1 12:00 vbmeta_b -> ../../sdf37
lrwxrwxrwx 1 root root   11 Jan  1 12:00 vbmeta_system_a -> ../../sdf17
lrwxrwxrwx 1 root root   11 Jan  1 12:00 vbmeta_system_b -> ../../sdf38
lrwxrwxrwx 1 root root   11 Jan  1 12:00 vbmeta_vendor_a -> ../../sdf18
lrwxrwxrwx 1 root root   11 Jan  1 12:00 vbmeta_vendor_b -> ../../sdf39
lrwxrwxrwx 1 root root   11 Jan  1 12:00 vendor_boot_a -> ../../sdf12
lrwxrwxrwx 1 root root   11 Jan  1 12:00 vendor_boot_b -> ../../sdf33
lrwxrwxrwx 1 root root   11 Jan  1 12:00 version_a -> ../../sdf19
lrwxrwxrwx 1 root root   11 Jan  1 12:00 version_b -> ../../sdf40
root@idcevo-hv-v920:/dev/disk/by-partlabel#
root@idcevo-hv-v920:/dev/disk/by-partlabel#cd
root@idcevo-hv-v920:~#
root@idcevo-hv-v920:~# dd if=/dev/sdf68 of=/tmp/disk.img
2101248+0 records in
2101248+0 records out
1075838976 bytes (1.1 GB, 1.0 GiB) copied, 8.18723 s, 131 MB/s
root@idcevo-hv-v920:~#
root@idcevo-hv-v920:~#
root@idcevo-hv-v920:~#
console:/ # ifconfig vnet32_0 10.23.0.20 up
console:/ # ip rule add pref 0 table main
console:/data/local/tmp  # nc -l -p 1234 > ramdump.disk
root@idcevo-hv-v920:~#nc 10.23.0.20 1234 < /tmp/disk.img
root@idcevo-hv-v920:~#
console:/ # setprop persist.vendor.usb.config adb
console:/ #

(After this step reboot the target, transfer the file to host via adb).
```

Enable IOC watchdog

To enable IOC watchdog on target, edit recovery-manager.in as below

patch for enabling IOC watchdog

```
add the below patch in /etc/recovery-manager.ini
EnableUserspaceWatchdog=false
EnableIocWatchdog=true
IocWatchdogTimeoutSec=30
IocWatchdogRatio=5
WatchdogDevice=/run/watchdog/swfi
```

> ⚠ **NOTE**: IOC watchdog applicable only for ci/cd builds.

Enable SOC watchdog

- enable soc watchdog dynamically via sysfs

```
echo 1 > /sys/devices/platform/dss/dss_panic_to_wdt.
```

> ⚠ SOC watchdog is not used in BMW CI/CD build

Ramdump - dss memory mapping

DSS have each domain memory area for saving dram raw data

.

<table>
<tr><td></td><td>Reserved 2MB</td><td></td><td></td></tr>
<tr><td>0xe1610000
0xe1210000</td><td>VM4 (16 MB)</td><td rowspan="2">0xe160fff
0xe1610000</td><td rowspan="2">VM3(16MB)</td></tr>
<tr><td>0xe060ffff
0xe0610000</td><td>VM2(60 MB)</td></tr>
</table>

Domain	section	start	Size	purpose	File
	Header	0xe0000000	64KB	DSS related dump	VM2_header_0xe0000000--0xe000ffff
	kernel	0xe0010000	2MB	bootloader & kernel log	VM2_kernel_0xe0010000--0xe020ffff
	platform	0xe0210000	4MB	platform	VM2_platform_0xe0210000--0xe060ffff

SYS(VM2)	kevents	0xe0810000	6MB	kernel event	VM2_kevent_0xe0810000--0xe0a0ffff
IVI (VM3)	Header	0xe1000000	64KB	DSS related dump	VM3_header_0xe1000000--0xe100ffff
	kernel	0xe1010000	2MB	bootloader & kernel log	VM3_kernel_0xe1010000--0xe120ffff
	platform	0xe1210000	4MB	platform	VM3_platform_0xe1210000--0xe160ffff
	kevents	0xe1810000	6MB	kernel event	VM3_kevent_0xe1810000--0xe1a0ffff

Ramdump - ufs partition details:

```
root@idcevo-hv-v920:~# ls -al /dev/disk/by-partlabel/
lrwxrwxrwx 1 root root   10 Jan  1 12:00 sfi_pbl_b -> ../../sde8
lrwxrwxrwx 1 root root   10 Jan  1 12:00 sfi_platform_a -> ../../sdd9
lrwxrwxrwx 1 root root   10 Jan  1 12:00 sfi_platform_b -> ../../sde9
lrwxrwxrwx 1 root root   11 Jan  1 12:00 smalldump -> ../../sdf68
lrwxrwxrwx 1 root root   10 Jan  1 12:00 strongbox_a -> ../../sdd5
lrwxrwxrwx 1 root root   10 Jan  1 12:00 strongbox_b -> ../../sde5
lrwxrwxrwx 1 root root   11 Jan  1 12:00 super -> ../../sdf60
lrwxrwxrwx 1 root root   11 Jan  1 12:00 superinactive -> ../../sdf61
```

```
lrwxrwxrwx 1 root root   11 Jan  1 12:00 smalldump -> ../../sdf68
```

Debugging

After collecting ramdump we can see multiple files out of these for kernel crash we can use vm2_kernel_xxxxxxxx.lst and vm3_kernel_xxxxxxxx.lst files for debugging kernel crash issues.

Name	Date modified	Type	Size
VM2_first_0xe0610000--0xe080ffff	17-08-2023 11:17	LST File	2,048 KB
VM2_header_0xe0000000--0xe000ffff	17-08-2023 11:17	LST File	64 KB
VM2_kernel_0xe0010000--0xe020ffff	17-08-2023 11:17	LST File	2,048 KB
VM2_kevent_0xe0810000--0xe0a0ffff	17-08-2023 11:17	LST File	2,048 KB
VM2_kmodule_0xe0e10000--0xe0e4ffff	17-08-2023 11:17	LST File	256 KB
VM2_platform_0xe0210000--0xe060ffff	17-08-2023 11:17	LST File	4,096 KB
VM3_first_0xe1610000--0xe180ffff	17-08-2023 11:17	LST File	2,048 KB
VM3_header_0xe1000000--0xe100ffff	17-08-2023 11:17	LST File	64 KB
VM3_kernel_0xe1010000--0xe120ffff	17-08-2023 11:17	LST File	2,048 KB
VM3_kevent_0xe1810000--0xe1a0ffff	17-08-2023 11:17	LST File	2,048 KB
VM3_kmodule_0xe1e10000--0xe1e4ffff	17-08-2023 11:17	LST File	256 KB
VM3_platform_0xe1210000--0xe160ffff	17-08-2023 11:17	LST File	4,096 KB
VM4_first_0xe2610000--0xe280ffff	17-08-2023 11:17	LST File	2,048 KB
VM4_header_0xe2000000--0xe200ffff	17-08-2023 11:17	LST File	64 KB
VM4_kernel_0xe2010000--0xe220ffff	17-08-2023 11:17	LST File	2,048 KB
VM4_kevent_0xe2810000--0xe2a0ffff	17-08-2023 11:17	LST File	2,048 KB
VM4_kmodule_0xe2e10000--0xe2e4ffff	17-08-2023 11:17	LST File	256 KB
VM4_platform_0xe2210000--0xe260ffff	17-08-2023 11:17	LST File	4,096 KB
VM5_header_0xe3000000--0xe300ffff	17-08-2023 11:17	LST File	64 KB
VM5_kernel_0xe3010000--0xe320ffff	17-08-2023 11:17	LST File	2,048 KB
VM5_platform_0xe3210000--0xe360ffff	17-08-2023 11:17	LST File	128 KB

- Based on panic that is from vm2 or from vm2 we can choose a file it will give the call traces of panic issue as shown below.

```
6>[   38.844685][   30.339978] [0:              sh:  348][  T348]sysrq: Trigger a crash
<0>[   38.845130][   30.340446] [0:              sh:  348][  T348]Kernel panic - not syncing: sysrq triggered
crash
<4>[   38.846654][   30.341949] [0:              sh:  348][  T348]CPU: 0 PID: 348 Comm: sh Not tainted 5.15.41 #1
<4>[   38.848162][   30.343444] [0:              sh:  348][  T348]Hardware name: BMW IDCEvo (v920-EVT0 SP21 B1)
Linux Sys VM (DT)
<4>[   38.848768][   30.344046] [0:              sh:  348][  T348]Call trace:
<4>[   38.849018][   30.344267] [0:              sh:  348][  T348] dump_backtrace+0x0/0x1f8
<4>[   38.850293][   30.345548] [0:              sh:  348][  T348] show_stack+0x20/0x30
<4>[   38.850538][   30.345783] [0:              sh:  348][  T348] dump_stack_lvl+0x68/0x84
<4>[   38.851824][   30.347063] [0:              sh:  348][  T348] dump_stack+0x18/0x34
<4>[   38.852063][   30.347302] [0:              sh:  348][  T348] panic+0x168/0x354
<4>[   38.852288][   30.347515] [0:              sh:  348][  T348] sysrq_handle_crash+0x24/0x28
<4>[   38.853585][   30.348806] [0:              sh:  348][  T348] __handle_sysrq+0x94/0x1a0
<4>[   38.853838][   30.349061] [0:              sh:  348][  T348] write_sysrq_trigger+0x13c/0x220
<4>[   38.874160][   30.369153] [0:              sh:  348][  T348] proc_reg_write+0xb0/0xf0
<4>[   38.874396][   30.369399] [0:              sh:  348][  T348] vfs_write+0xc8/0x388
<4>[   38.875637][   30.370634] [0:              sh:  348][  T348] ksys_write+0x74/0x100
<4>[   38.875846][   30.370841] [0:              sh:  348][  T348] __arm64_sys_write+0x24/0x30
<4>[   38.876081][   30.371068] [0:              sh:  348][  T348] invoke_syscall+0x74/0xf0
<12>[   38.894299][   30.389069] [
```

- from the above trace, for example if we consider backtrace+0x0/0x1f8 this offset address can be decoded with vmlinux with the below command.
- And vmlinux will be available in the artifactory images itself.
- Download toolchain,give the path of toolchain and vmlinux press enter it will enter into gdb mode.

/data/home/vkenche/workspace/Tool_Chain_Copied/sysroots/x86_64-pokysdk-linux/usr/bin/aarch64-poky-linux/aarch64-poky-linux-gdb vmlinux

```
(gdb) list *(backtrace+0x0)
```

How to align ramdump extraction tool with DSS offset

- Here we can find the size of each section in dss kernel/include/dt-bindings/soc/samsung/exynosauto9-debug.h.
- evt0 is picking from /sources/linux_sys_dts-la/linux_sys/exynosautov920-sadk-en-debug.dtsi memory regions can be modified from here and with above header file.

How to handle - Kernel crashed but no warm reset from IOC:

- [General Information] Ramdump logs are present in RAM, as long as the target has Power, all the Ramdump logs are present in Target RAM.
- During issue when the target is stuck (and control is not Automatically going to LK), **press Middle-Button of Debug-Adapter-Pro or Pro-Low** (no t applicable to Debug-Adapter-Lite).
    1. Pressing middle button will only RESET Target, Power is not cut. Hence, Issue time Ramdump logs are present in Target RAM.
- Immediately press “S” to stop at LK and then run command “fast” to enter fastboot mode.
- Now you can take full ramdump, by running in host command “python eautodump.py”

SOFTLOCKUP:

The Linux kernel can act as a watchdog to detect both soft and hard lockups.

A ‘softlockup’ is defined as a bug that causes the kernel to loop in kernel mode for more than 20 seconds without giving other tasks a chance to run.

Soft lockup is triggered with Linux kernel Dump Test Module(LKDTM).

soft lockup is triggered by below commands.

```
# insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkdtm.ko
# echo SOFTLOCKUP > /sys/kernel/debug/provoke-crash/DIRECT
```

```
root@idcevo-hw-v920:~# ls
adb.sh  diag-monitor  host.sh  ree_tests  uppercase
root@idcevo-hw-v920:~# insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkdtm.ko
root@idcevo-hw-v920:~# echo SOFTLOCKUP > /sys/kernel/debug/provoke-crash/DIRECT
[  116.012390][    C1] watchdog: BUG: soft lockup - CPU#1 stuck for 45s! [sh:297]
[  116.014352][    C1] Kernel panic - not syncing: softlockup: hung tasks
[  116.015848][    C1] CPU: 1 PID: 297 Comm: sh Tainted: G             L    5.15.41 #1
[  116.016419][    C1] Hardware name: BMW IDCEvo (SP21-v920-B1) Linux Sys VM (DT)
[  116.017892][    C1] Call trace:
[  116.018054][    C1]  dump_backtrace+0x0/0x1c0
[  116.019299][    C1]  show_stack+0x18/0x28
[  116.019505][    C1]  dump_stack_lvl+0x68/0x84
[  116.019725][    C1]  dump_stack+0x18/0x34
[  116.020946][    C1]  panic+0x160/0x34c
[  116.021139][    C1]  watchdog_timer_fn+0x264/0x2c0
[  116.041215][    C1]  __hrtimer_run_queues+0x148/0x320
[  116.041475][    C1]  hrtimer_interrupt+0xf4/0x250
[  116.042734][    C1]  arch_timer_handler_virt+0x34/0x48
[  116.042999][    C1]  handle_percpu_devid_irq+0xa0/0x240
[  116.044289][    C1]  handle_domain_irq+0x90/0xd8
[  116.064311][    C1]  gic_handle_irq+0x54/0x120
[  116.064544][    C1]  call_on_irq_stack+0x28/0x50
[  116.065797][    C1]  do_interrupt_handler+0x54/0x60
[  116.066052][    C1]  el1_interrupt+0x30/0x78
[  116.066290][    C1]  el1h_64_irq_handler+0x18/0x28
[  116.086370][    C1]  el1h_64_irq+0x7c/0x80
[  116.086584][    C1]  lkdtm_SOFTLOCKUP+0x14/0x20 [lkdtm]
[  116.087877][    C1]  lkdtm_do_action+0xic/0x30 [lkdtm]
[  116.088135][    C1]  direct_entry+0xe0/0x148 [lkdtm]
[  116.089414][    C1]  full_proxy_write+0x60/0xb0
[  116.109485][    C1]  vfs_write+0xc0/0x380
[  116.109694][    C1]  ksys_write+0x6c/0xf8
[  116.109898][    C1]  __arm64_sys_write+0x1c/0x28
[  116.111125][    C1]  invoke_syscall+0x44/0x108
[  116.111357][    C1]  el0_svc_common.constprop.0+0xcc/0xf0
```

Attached the complete log.

softlock_up_txt

Ramdump sys_kernel log

SYS_kernel_0xe001...0--0xe020ffff.lst

Hard Lockup :

A ‘hardlockup’ is defined as a bug that causes the CPU to loop in kernel mode for more than 10 seconds, without letting other interrupts have a chance to run.

Hard lockup is triggered with Linux kernel Dump Test Module(LKDTM).

Below are the steps to trigger hard LOCKUP

```
# insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkdtm.ko
# echo HARDLOCKUP > /sys/kernel/debug/provoke-crash/DIRECT
```

Driver Path

HardLOCKUP Detector: kernel/drivers/soc/samsung/debug/hardlockup-watchdog.c

HardLOCKUP Generation: kernel/drivers/misc/lkdtm

Attached the console log

hardlockup_es1.txt

Ramdump sys_kernel log

SYS_kernel_0xe001...0--0xe020ffff.lst

.

Hung_Task:

The hung task is detected by linux kernel by parsing processes with uninterruptible sleep state(which are waiting for some event or resource and is usually not going to move forward) for long time and which are stalled into this D state.

```
echo HUNG_TASK > /sys/kernel/debug/provoke-crash/DIRECT
```

root@idcevo-hv-v920:~# zcat /proc/config.gz | grep HUNG_TASK
CONFIG_DETECT_HUNG_TASK=y
CONFIG_DEFAULT_HUNG_TASK_TIMEOUT=120
CONFIG_BOOTPARAM_HUNG_TASK_PANIC=y
CONFIG_BOOTPARAM_HUNG_TASK_PANIC_VALUE=1

hung_task_panic_value If set to 1, the kernel panics if any user or kernel thread sleeps in the TASK_UNINTERRUPTIBLE state (D state) for more than HUNG_TASK_TIMEOUT seconds. A process remains in D state while waiting for I/O to complete. You cannot kill or interrupt a process in this state.

```
root@idcevo-hv-v920:~# zcat /proc/config.gz  | grep HUNG_TASK
CONFIG_DETECT_HUNG_TASK=y
CONFIG_DEFAULT_HUNG_TASK_TIMEOUT=120
CONFIG_BOOTPARAM_HUNG_TASK_PANIC=y
CONFIG_BOOTPARAM_HUNG_TASK_PANIC_VALUE=1
root@idcevo-hv-v920:~# insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkdtm.ko
root@idcevo-hv-v920:~# echo HUNG_TASK > /sys/kernel/debug/provoke-crash/DIRECT
[  725.983683][   T30] INFO: task sh:295 blocked for more than 120 seconds.
[  725.985320][   T30]       Not tainted 5.15.41 #1
[  725.985887][   T30] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.
[  725.987671][   T30] task:sh              state:D stack:    0 pid:  295 ppid:     1 flags:0x00000200
[  725.989327][   T30] Call trace:
[  725.989498][   T30]  __switch_to+0x10c/0x1c8
[  725.989741][   T30]  __schedule+0x330/0x9f8
[  725.990991][   T30]  schedule+0x44/0xf8
[  725.991196][   T30]  lkdtm_HUNG_TASK+0x2c/0x38 [lkdtm]
[  725.992585][   T30]  lkdtm_do_action+0x1c/0x30 [lkdtm]
[  725.992876][   T30]  direct_entry+0xe0/0x148 [lkdtm]
[  726.013076][   T30]  full_proxy_write+0x60/0xb0
[  726.013350][   T30]  vfs_write+0xc0/0x380
[  726.014592][   T30]  ksys_write+0x6c/0xf8
[  726.014803][   T30]  __arm64_sys_write+0x1c/0x28
[  726.015039][   T30]  invoke_syscall+0x44/0x108
[  726.035215][   T30]  el0_svc_common.constprop.0+0xcc/0xf0
[  726.035603][   T30]  do_el0_svc+0x24/0x88
[  726.036850][   T30]  el0_svc+0x20/0x60
[  726.037048][   T30]  el0t_64_sync_handler+0xb0/0xb8
[  726.037293][   T30]  el0t_64_sync+0x1a4/0x1a8
[  726.057510][   T30] Kernel panic - not syncing: hung_task: blocked tasks
[  726.057875][   T30] CPU: 1 PID: 30 Comm: khungtaskd Not tainted 5.15.41 #1
[  726.059248][   T30] Hardware name: BMW IDCEvo (SP21-v920-B1) Linux Sys VM (DT)
[  726.060643][   T30] Call trace:
[  726.080587][   T30]  dump_backtrace+0x0/0x1c0
[  726.080831][   T30]  show_stack+0x18/0x28
[  726.081054][   T30]  dump_stack_lvl+0x68/0x84
T30]  dump_st][
ack+0x18/0Broadcx34
```

Attached the complete log.

hung_task_sys.txt

Ramdump sys_kernel log

SYS_kernel_0xe001...0--0xe020ffff.lst

Panic:

echo PANIC > /sys/kernel/debug/provoke-crash/DIRECT

```
root@idcevo-hw-v920:~#
root@idcevo-hw-v920:~# DIRECT
-sh: DIRECT: command not found
root@idcevo-hw-v920:~# echo PANIC > /sys/kernel/debug/provoke-crash/DIRECT
[   94.590089][  T297] Kernel panic - not syncing: dumptest
[   94.600605][  T297] CPU: 1 PID: 297 Comm: sh Not tainted 5.15.41 #1
[   94.601123][  T297] Hardware name: BMW IDCEvo (SP21-v920-B1) Linux Sys VM (DT)
[   94.602522][  T297] Call trace:
[   94.602788][  T297]  dump_backtrace+0x0/0x1c0
[   94.604154][  T297]  show_stack+0x18/0x28
[   94.604380][  T297]  dump_stack_lvl+0x68/0x84
[   94.605644][  T297]  dump_stack+0x18/0x34
[   94.605857][  T297]  panic+0x160/0x34c
[   94.606063][  T297]  lkdtm_EXHAUST_STACK+0x0/0x4c [lkdtm]
[   94.607380][  T297]  lkdtm_do_action+0xic/0x30 [lkdtm]
[   94.607665][  T297]  direct_entry+0xe0/0x148 [lkdtm]
[   94.627748][  T297]  full_proxy_write+0x60/0xb0
[   94.628003][  T297]  vfs_write+0xc0/0x380
[   94.629250][  T297]  ksys_write+0x6c/0xf8
[   94.629458][  T297]  __arm64_sys_write+0x1c/0x28
[   94.629697][  T297]  invoke_syscall+0x44/0x108
[   94.649752][  T297]  el0_svc_common.constprop.0+0xcc/0xf0
[   94.650035][  T297]  do_el0_svc+0x24/0x88
[   94.651269][  T297]  el0_svc+0x20/0x60
[   94.651471][  T297]  el0t_64_sync_handler+0xb0/0xb8
[   94.651719][  T297]  el0t_64_sync+0x1a4/0x1a8
[   94.671780][  T297] SMP: stopping secondary CPUs
[   94.672065][    C2] debug-snapshot dss: core register saved(CPU:2)
[   94.673507][    C2] debug-snapshot dss: context saved(CPU:2)
[   94.673808][    C2] CPU: 2 PID: 0 Comm: swapper/2 Not tainted 5.15.41 #1
[   94.675162][    C2] Hardware name: BMW IDCEvo (SP21-v920-B1) Linux Sys VM (DT)
[   94.695285][    C2] Call trace:
[   94.695435][    C2]  dump_backtrace+0x0/0x1c0
[   94.696674][    C2]  show_stack+0x18/0x28
[   94.696857][    C2]  dump_stack_lvl+0x68/0x84
[   94.716845][    C2]  dump_stack+0x18/0x34
[   94.717031][    C2]  dbg_snapshot_save_context+0x214/0x218
[   94.718299][    C2]  dbg_snapshot_ipi_stop+0x24/0x30
[   94.718518][    C2]  __traceiter_android_vh_ipi_stop+0x38/0x58
[   94.719800][    C2]  ipi_handler+0x2f0/0x340
[   94.739822][    C2]  handle_percpu_devid_irq+0xa0/0x240
[   94.740055][    C2]  handle_domain_irq+0x90/0xd8
[   94.741284][    C2]  gic_handle_irq+0x54/0x120
[   94.741486][    C2]  call_on_irq_stack+0x28/0x50
[   94.761524][    C2]  do_interrupt_handler+0x54/0x60
[   94.761744][    C2]  el1_interrupt+0x30/0x78
```

Attached the console log

kernel_panic_log.txt

Ramdump log

SYS_kernel_0xe001...0--0xe020ffff.lst

Spinlockup:

In the Mutex concept, when the thread is trying to lock or acquire the Mutex which is not available then that thread will go to sleep until that Mutex is available. Whereas in Spinlock it is different. The spinlock is a very simple single-holder lock. If a process attempts to acquire a spinlock and it is unavailable, the process will keep trying (spinning) until it can acquire the lock. This simplicity creates a small and fast lock.

```
echo SPINLOCKUP > /sys/kernel/debug/provoke-crash/DIRECT
```

Attached the complete log.

Ramdump log

spinlock_sys_log.txt

SYS_kernel_0xe001...0--0xe020ffff.lst

Release	ES1
HW	SP21
IVI	

Soft Lockup :

Soft lockup is triggered with Linux kernel Dump Test Module(LKDTM).

For this need to enable two configs

```
CONFIG_BOOTPARAM_SOFTLOCKUP_PANIC=y
CONFIG_BOOTPARAM_SOFTLOCKUP_PANIC_VALUE=1
```

Verified the back traces with softlock its generating the back traces which causes the crash we can see that with below image. For analyzing with ramdump need a separate tool because it's in binary format.

```
console:/ #
console:/ # zcat /pr
proc/     product/
console:/ # zcat /proc/config.gz | grep BOOTPARAM_SOFTLOCKUP_PANIC
CONFIG_BOOTPARAM_SOFTLOCKUP_PANIC=y
CONFIG_BOOTPARAM_SOFTLOCKUP_PANIC_VALUE=1
console:/ # echo SOFTLOCKUP > /sys/kernel/debug/provoke-crash/DIRECT
[  116.019463][    C4] watchdog: BUG: soft lockup - CPU#4 stuck for 45s! [sh:322]
[  116.021772][    C4] Kernel panic - not syncing: softlockup: hung tasks
[  116.022250][    C4] CPU: 4 PID: 322 Comm: sh Tainted: G            EL    5.15.41-android13-8-gae7a8acd6a89-dirty #1
[  116.023922][    C4] Hardware name: BMW IDCEvo (SP21-v920-B1) Android IVI VM (DT)
[  116.025268][    C4] Call trace:
[  116.025397][    C4]  dump_backtrace+0x0/0x1d4
[  116.026602][    C4]  show_stack+0x1c/0x2c
[  116.026767][    C4]  dump_stack_lvl+0x68/0x84
[  116.026946][    C4]  dump_stack+0x1c/0x40
[  116.028141][    C4]  panic+0x164/0x3a8
[  116.028297][    C4]  watchdog_timer_fn+0x224/0x230
[  116.048394][    C4]  __run_hrtimer+0xa8/0x26c
[  116.048577][    C4]  hrtimer_interrupt+0x1e4/0x2cc
[  116.049797][    C4]  arch_timer_handler_virt+0x40/0x54
[  116.050013][    C4]  handle_percpu_devid_irq+0x88/0x21c
[  116.070151][    C4]  handle_domain_irq+0x60/0xa8
[  116.070342][    C4]  gic_handle_irq+0x54/0x12c
[  116.071551][    C4]  call_on_irq_stack+0x40/0x70
[  116.071745][    C4]  do_interrupt_handler+0x40/0x58
[  116.073021][    C4]  el1_interrupt+0x34/0x60
[  116.092999][    C4]  el1h_64_irq_handler+0x1c/0x2c
[  116.093199][    C4]  el1h_64_irq+0x7c/0x80
[  116.094398][    C4]  lkdtm_SOFTLOCKUP+0x14/0x1c
[  116.094589][    C4]  direct_entry+0x11c/0x12c
[  116.094768][    C4]  full_proxy_write+0x70/0xf8
[  116.114782][    C4]  vfs_write+0xf8/0x33c
[  116.114958][    C4]  ksys_write+0x7c/0xec
[  116.115132][    C4]  __arm64_sys_write+0x20/0x30
[  116.116320][    C4]  invoke_syscall+0x44/0x120
[  116.116506][    C4]  el0_svc_common+0xb8/0xf8
[  116.136557][    C4]  do_el0_svc+0x28/0x88
[  116.136733][    C4]  el0_svc+0x24/0x84
[  116.136890][    C4]  el0t_64_sync_handler+0x88/0xec
```

Attached the complete log.

softlock_ivi.txt

Hard Lockup :

Hard lockup is triggered with Linux kernel Dump Test Module(LKDTM).

Below are the steps to trigger hard LOCKUP in IVI

CONFIG_LKDTM=y this config should be enabled for this there are two dependencies as mentioned below.

```
#CONFIG_RUNTIME_TESTING_MENU=y
#CONFIG_DEBUG_FS=y
```

Verified Back traces with hardlock crash its generating the appropriate function call which causing the panic.

```
console:/ $ su
console:/ #
console:/ #
console:/ # echo HARDLOCKUP > /sys/kernel/debug/provoke-crash/DIRECT
[   26.741142][    C4] Kernel panic - not syncing: Watchdog detected hard LOCKUP on cpu 5
[   26.742747][    C4] CPU: 4 PID: 0 Comm: swapper/4 Tainted: G            E     5.15.41-android13-8-gae7a8acd6a89-dirty #1
[   26.744456][    C4] Hardware name: BMW IDCEvo (SP21-v920-B1) Android IVI VM (DT)
[   26.746230][    C4] Call trace:
[   26.746368][    C4]  dump_backtrace+0x0/0x1d4
[   26.746561][    C4]  show_stack+0x1c/0x2c
[   26.747759][    C4]  dump_stack_lvl+0x68/0x84
[   26.747949][    C4]  dump_stack+0x1c/0x40
[   26.748117][    C4]  panic+0x164/0x3a8
[   26.749301][    C4]  hardlockup_stop_fn+0x0/0xe0 [hardlockup_watchdog]
[   26.749572][    C4]  __run_hrtimer+0xa8/0x26c
[   26.769602][    C4]  hrtimer_interrupt+0x1e4/0x2cc
[   26.769809][    C4]  arch_timer_handler_virt+0x40/0x54
[   26.771059][    C4]  handle_percpu_devid_irq+0x88/0x21c
[   26.771284][    C4]  handle_domain_irq+0x60/0xa8
[   26.791293][    C4]  gic_handle_irq+0x54/0x12c
[   26.791483][    C4]  call_on_irq_stack+0x40/0x70
[   26.792701][    C4]  do_interrupt_handler+0x40/0x58
[   26.792905][    C4]  el1_interrupt+0x34/0x60
[   26.793090][    C4]  el1h_64_irq_handler+0x1c/0x2c
[   26.813145][    C4]  el1h_64_irq+0x7c/0x80
[   26.813321][    C4]  arch_local_irq_enable+0xc/0x18
[   26.814552][    C4]  default_idle_call+0x3c/0x14c
[   26.814752][    C4]  do_idle+0x100/0x298
[   26.814929][    C4]  cpu_startup_entry+0x28/0x2c
[   26.834994][    C4]  secondary_start_kernel+0x194/0x1cc
[   26.835214][    C4]  __secondary_switched+0x98/0x9c
[   26.836444][    C4] SMP: stopping secondary CPUs
[   26.836680][    C0] debug-snapshot dss: core register saved(CPU:0)
[   26.856754][    C0] debug-snapshot dss: context saved(CPU:0)
[   26.857011][    C0] CPU: 0 PID: 0 Comm: swapper/0 Tainted: G            E     5.15.41-android13-8-gae7a8acd6a89-dirty #1
[   26.858487][    C0] Hardware name: BMW IDCEvo (SP21-v920-B1) Android IVI VM (DT)
[   26.878625][    C0] Call trace:
[   26.878758][    C0]  dump_backtrace+0x0/0x1d4
[   26.879993][    C0]  show_stack+0x1c/0x2c
[   26.880162][    C0]  dump_stack_lvl+0x68/0x84
[   26.880356][    C0]  dump_stack+0x1c/0x40
[   26.900353][    C0]  dbg_snapshot_save_context+0x2b0/0x2bc [dss]
[   26.900661][    C0]  dbg_snapshot_ipi_stop+0x28/0x38 [dss]
[   26.901926][    C0]  __traceiter_android_vh_ipi_stop+0x34/0x54
[   26.902171][    C0]  do_handle_IPI+0x184/0x1a4
[   26.922137][    C0]  ipi_handler+0x20/0x34
[   26.922313][    C0]  handle_percpu_devid_irq+0x88/0x21c
[   26.923557][    C0]  handle_domain_irq+0x60/0xa8
[   26.923745][    C0]  gic_handle_irq+0x54/0x12c
[   26.923930][    C0]  call_on_irq_stack+0x40/0x70
```

Attached the complete log.

hardlock_ramdump_ivi.txt

KEVENT:

pase kevent log through keventparser.

keventparser parses kevent area with System.map of kernel to get symbol name of kernel.

the tool is in "sources/tool/ramdump/keventparser/src"

you can build with "make"

./parser -k kevent.log -m System.map > out.txt

For example:

./parser -k VM3_kevent_0xe1810000--0xe1a0ffff.lst -m System.map > out.txt

out.txt

LKDTM testing

SYS side

Tried crash-> ramdump with latest ES1.sys files built, on top of COCKPIT_ARTIFACTS_92.

tried with the command, "insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkdtm.ko cpoint_name=DIRECT cpoint_type=<*CRASHTYPE*>"

CRASHTYPE(BUG) => ramdump is generated.

bug_log.txt

```
[  823.681982][  T460] x2 : ffffff8a18cd68a8 x1 : ffffffc000f73010 x0 : ffffffc000f6e7a8
[  823.683343][  T460] Call trace:
[  823.703306][  T460]  lkdtm_BUG+0x0/0x8 [lkdtm]
[  823.703528][  T460]  lkdtm_register_cpoint+0x74/0x98 [lkdtm]
[  823.704800][  T460]  lkdtm_module_init+0x194/0x1fc [lkdtm]
[  823.705043][  T460]  do_one_initcall+0x48/0x288
[  823.705258][  T460]  do_init_module+0x48/0x1f8
[  823.725309][  T460]  load_module+0x2174/0x2850
[  823.725512][  T460]  __do_sys_finit_module+0xb8/0xf8
[  823.726810][  T460]  __arm64_sys_finit_module+0x20/0x30
[  823.727049][  T460]  invoke_syscall+0x44/0x108
[  823.727257][  T460]  el0_svc_common.constprop.0+0xcc/0xf0
[  823.747315][  T460]  do_el0_svc+0x24/0x88
[  823.747504][  T460]  el0_svc+0x20/0x60
[  823.748712][  T460]  el0t_64_sync_handler+0xb0/0xb8
[  823.748931][  T460]  el0t_64_sync+0x1a4/0x1a8
[  823.749129][  T460] Code: d65f03c0 52800020 d50323bf d65f03c0 (d4210000)
[  823.769231][  T460] ---[ end trace 89c8a72751d25966 ]---
[  823.769491][  T460] Kernel panic - not syncing: Oops - BUG: Fatal exception
```

CRASHTYPE(EXCEPTION) => ramdump is generated

```
[   40.473101][  T449] x2 : ffffff8a0d94dc10 x1 : ffffffc000f73040 x0 : 0000000000000000
[   40.493316][  T449] Call trace:
[   40.493461][  T449]  lkdtm_EXCEPTION+0xc/0x18 [lkdtm]
[   40.494721][  T449]  lkdtm_register_cpoint+0x74/0x98 [lkdtm]
[   40.494981][  T449]  lkdtm_module_init+0x194/0x1fc [lkdtm]
[   40.515092][  T449]  do_one_initcall+0x48/0x288
[   40.515307][  T449]  do_init_module+0x48/0x1f8
[   40.516538][  T449]  load_module+0x2174/0x2850
[   40.516737][  T449]  __do_sys_finit_module+0xb8/0xf8
[   40.517981][  T449]  __arm64_sys_finit_module+0x20/0x30
[   40.538061][  T449]  invoke_syscall+0x44/0x108
[   40.538265][  T449]  el0_svc_common.constprop.0+0xcc/0xf0
[   40.539524][  T449]  do_el0_svc+0x24/0x88
[   40.539709][  T449]  el0_svc+0x20/0x60
[   40.559788][  T449]  el0t_64_sync_handler+0xb0/0xb8
[   40.560004][  T449]  el0t_64_sync+0x1a4/0x1a8
[   40.561279][  T449] Code: d65f03c0 d2800000 d503233f d50323bf (b900001f)
[   40.561592][  T449] ---[ end trace 55e84dd6e1c6576b ]---
[   40.562864][  T449] Kernel panic - not syncing: Oops: Fatal exception
[   40.582934][  T449] SMP: stopping secondary CPUs
```

exception_log.txt

CRASHTYPE(EXHAUST_STACK) =>ramdump. stuck at kevents

exhaust_stack_log.txt

```
3 0:[   41.695478][    C0]        0                 0                 0                 0 RK   0> 0                 0 ffffffc00a0bf080 *         swapper/0
3 0:[   41.698022][    C0] Call trace:
3 0:[   41.717988][    C0]  dump_backtrace+0x0/0x1d4
3 0:[   41.718171][    C0]  dbg_snapshot_dump_one_task_info+0x1a8/0x1e0 [dss]
3 0:[   41.719489][    C0]  dbg_snapshot_post_panic_handler+0x340/0x500 [dss]
3 0:[   41.719769][    C0]  atomic_notifier_call_chain+0x54/0x94
3 0:[   41.739760][    C0]  panic+0x18c/0x3a8
3 0:[   41.739928][    C0]  _panic_trigger_sysconf+0xc0/0xf80 [vlx_panic_trigger_module]
3 0:[   41.741242][    C0]  xirq_handler+0x1c/0x30 [vlx_hyp_module]
3 0:[   41.741486][    C0]  __handle_irq_event_percpu+0x88/0x220
3 0:[   41.761529][    C0]  handle_irq_event+0x64/0x144
3 0:[   41.761721][    C0]  handle_fasteoi_irq+0x110/0x210
3 0:[   41.762946][    C0]  handle_domain_irq+0x60/0xa8
3 0:[   41.782927][    C0]  gic_handle_irq+0x54/0x12c
3 0:[   41.783115][    C0]  call_on_irq_stack+0x40/0x70
3 0:[   41.784330][    C0]  do_interrupt_handler+0x40/0x58
3 0:[   41.784529][    C0]  el1_interrupt+0x34/0x60
3 0:[   41.784706][    C0]  el1h_64_irq_handler+0x1c/0x2c
3 0:[   41.804704][    C0]  el1h_64_irq+0x7c/0x80
3 0:[   41.804878][    C0]  arch_local_irq_enable+0xc/0x18
3 0:[   41.806106][    C0]  default_idle_call+0x3c/0x14c
3 0:[   41.806299][    C0]  do_idle+0x100/0x298
3 0:[   41.826277][    C0]  cpu_startup_entry+0x28/0x2c
3 0:[   41.826469][    C0]  rest_init+0xe4/0xf8
3 0:[   41.826634][    C0]  arch_call_rest_init+0x14/0x24
3 0:[   41.827831][    C0]  start_kernel+0x37c/0x494
3 0:[   41.847803][    C0]  __primary_switched+0xc4/0xcc
```

CRASHTYPE(CORRUPT_STACK) => **dss, no reboot.on restart, no ram dump.**

corrupt_stak_log.txt

```
[   82.283957][  T447] Kernel panic - not syncing: stack-protector: Kernel stack is corrupted in: lkdtm_CORRUPT_STACK+0x48/0x58 [lkdtm]
[   82.285942][  T447] CPU: 2 PID: 447 Comm: insmod Not tainted 5.15.41 #1
[   82.287445][  T447] Hardware name: BMW IDCEvo (SP21-v920-B1) Linux Sys VM (DT)
[   82.288987][  T447] Call trace:
[   82.289142][  T447]  dump_backtrace+0x0/0x1c0
[   82.289369][  T447]  show_stack+0x18/0x28
[   82.290593][  T447]  dump_stack_lvl+0x68/0x84
[   82.290882][  T447]  dump_stack+0x18/0x34
[   82.290986][  T447]  panic+0x160/0x34c
[   82.292184][  T447]  __stack_chk_fail+0x30/0x40
[   82.292399][  T447]  lkdtm_CORRUPT_STACK+0x48/0x58 [lkdtm]
[   82.312482][  T447]  lkdtm_do_action+0x1c/0x30 [lkdtm]
[   82.312731][  T447]  0xffffffffffffffff
[   82.313945][  T447] SMP: stopping secondary CPUs
[   82.314204][    C0] debug-snapshot dss: core register saved(CPU:0)
[   82.315669][    C0] debug-snapshot dss: context saved(CPU:0)
[   82.335745][    C0] CPU: 0 PID: 0 Comm: swapper/0 Not tainted 5.15.41 #1
[   82.336113][    C0] Hardware name: BMW IDCEvo (SP21-v920-B1) Linux Sys VM (DT)
```

CRASHTYPE(WRITE_AFTER_FREE), => no crash

write_after_free_log.txt

```
[1] 0:console1:/ $ root@idcevo-hw-v920:~# insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkdtm.ko cpoint_name=DIRECT cpoint_type=WRITE_AFTER_FREE
root@idcevo-hw-v920:~# dmesg
```

CRASHTYPE(READ_AFTER_FREE),=> no crash

read_after_free_log.txt

```
root@idcevo-hw-v920:~# insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkdtm.ko cpoint_name=DIRECT cpoint_type=READ_AFTER_FREE
root@idcevo-hw-v920:~#
root@idcevo-hw-v920:~#
root@idcevo-hw-v920:~#
```

CRASHTYPE(HUNG_TASK), => dss, no reboot.on restart, no ram dump.

hung_task_log.txt

CRASHTYPE(EXEC_KMALLOC) => ramdump. stuck at kevents
CRASHTYPE(EXEC_VMALLOC) => ramdump. stuck at kevents
CRASHTYPE(USERCOPY_KERNEL) => ramdump

Many time ramdump is stop at kevents dumping. with following message.

./20221229-1710_virt_from_dram/SYS_kevents_0xe2b50000--0xe314ffff.lst...
_command_receive, resp is strage, forcely go

Attaching current sys logs with stack trace.

crash_logs.zip

IVI Testing

Following commands for lkdtm on android.

console:/ # rmmod lkdtm.ko
console:/ # insmod /vendor_dlkm/lib/modules/lkdtm.ko cpoint_name=DIRECT cpoint_type=HUNG_TASK

Below are the logs.

CRASHTYPE(BUG) => ramdump

and_bug_log.txt

```
console:/ # rmmod lkdtm.ko
console:/ # insmod /vendor_dlkm/lib/modules/lkdtm.ko cpoint_name=DIRECT cpoint>
[   78.785091][ T3540] kernel BUG at drivers/misc/lkdtm/bugs.c:76!
[   78.786691][ T3540] Internal error: Oops - BUG: 0 [#1] PREEMPT SMP
[   78.787258][ T3540] debug-snapshot dss: core register saved(CPU:4)
[   78.788686][ T3540] debug-snapshot dss: context saved(CPU:4)
[   78.789074][ T3540] item - log_kevents is disabled
[   78.790329][ T3540]
```

CRASHTYPE(EXCEPTION) => ramdump

and_exception_log.txt

```
console:/ # rmmod lkdtm.ko
p_dlkm/lib/modules/lkdtm.ko cpoint_name=DIRECT cpoint_type=EXCEPTION          <
[  115.905052][ T4189] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000
[  115.907223][ T4189] Mem abort info:
[  115.907541][ T4189]   ESR = 0x96000045
[  115.908815][ T4189]   EC = 0x25: DABT (current EL), IL = 32 bits
[  115.909391][ T4189]   SET = 0, FnV = 0
[  115.909659][ T4189]   EA = 0, S1PTW = 0
[  115.910821][ T4189]   FSC = 0x05: level 1 translation fault
[  115.911042][ T4189] Data abort info:
[  115.912209][ T4189]   ISV = 0, ISS = 0x00000045
[  115.912400][ T4189]   CM = 0, WnR = 1
[  115.912549][ T4189] user pgtable: 4k pages, 39-bit VAs, pgdp=000000091618b000
[  115.914159][ T4189] [0000000000000000] pgd=0000000000000000, p4d=0000000000000000, pud=0000000000000000
[  115.934530][ T4189] Internal error: Oops: 96000045 [#1] PREEMPT SMP
[  115.936080][ T4189] debug-snapshot dss: core register saved(CPU:6)
[  115.936331][ T4189] debug-snapshot dss: context saved(CPU:6)
[  115.956402][ T4189] item - log_kevents is disabled
[  115.956641][ T4189]
```

CRASHTYPE(EXHAUST_STACK) =>ramdump

and_EXHAUST_STACK_log.txt

```
console:/ # rmmod lkdtm.ko
p_dlkm/lib/modules/lkdtm.ko cpoint_name=DIRECT cpoint_type=EXHAUST_STACK      <
[  282.335228][    C6] Insufficient stack space to handle exception!
[  282.335229][    C6] ESR: 0x96000047 -- DABT (current EL)
[  282.335235][    C6] FAR: 0xffffffc018f5fre0
[  282.335241][    C6] Task stack:     [0xffffffc018f60000..0xffffffc018f64000]
[  282.335248][    C6] IRQ stack:      [0xffffffc08a378000..0xffffffc08a37c000]
[  282.335254][    C6] Overflow stack: [0xffffff87ee7e3110..0xffffff87ee7e4110]
[  282.335261][    C6] CPU: 6 PID: 7072 Comm: insmod Tainted: G        E     5.15.41-android13-8-gd10b75b8b12b #1
[  282.335276][    C6] Hardware name: BMW IDCEvo (SP21-v920-B1) Android IVI VM (DT)
[  282.335285][    C6] pstate: 20400005 (nzCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--)
[  282.335296][    C6] pc : sched_clock+0x8/0x60
[  282.335327][    C6] lr : vprintk_store+0xb0/0x72c
[  282.335345][    C6] sp : ffffffc018f60010
[  282.335351][    C6] x29: ffffffc018f60010 x28: ffffffc08a15050 x27: ffffffc0018a61d8
[  282.335363][    C6] x26: 0000000000000000 x25: 0000000ffffffff x24: ffffffc018f0138
[  282.335371][    C6] x23: 0000000000000000 x22: ffffffc001bb5e11 x21: 0000000000001ba0
[  282.335379][    C6] x20: 0000000000000000 x19: 0000000ffffffff x18: ffffffc00d51980
[  282.335384][    C6] x17: ffffffc018f602aa x16: ffffffffffffffff x15: 0000000000000004
[  282.335393][    C6] x14: ffffff87ee4f5000 x13: 0000000000007915 x12: 0000000000000001
[  282.335399][    C6] x11: 0000000000000000 x10: 0000000000000000 x9 : 0000000000000000
[  282.335407][    C6] x8 : ffffff8e33c3400 x7 : 1414141414141414 x6 : 000000000000001f
[  282.335413][    C6] x5 : 0000000000000040 x4 : ffffffc018f60138 x3 : ffffffc001bb5e11
[  282.335420][    C6] x2 : 0000000000000000 x1 : 0000000ffffffff x0 : 0000000000000000
[  282.335430][    C6] Kernel panic - not syncing: kernel stack overflow
[  282.335439][    C6] CPU: 6 PID: 7072 Comm: insmod Tainted: G        E     5.15.41-android13-8-gd10b75b8b12b #1
[  282.335447][    C6] Hardware name: BMW IDCEvo (SP21-v920-B1) Android IVI VM (DT)
[  282.335454][    C6] Call trace:
[  282.335460][    C6]  dump_backtrace+0x0/0x1d4
[  282.335475][    C6]  show_stack+0x1c/0x2c
[  282.335479][    C6]  dump_stack_lvl+0x68/0x84
[  282.335493][    C6]  dump_stack+0x18/0x30
[  282.335499][    C6]  panic+0x1d4/0x3c0
[  282.335500][    C6]  test_taint+0x0/0x24
[  282.335511][    C6]  panic_bad_stack+0x108/0x11c
[  282.335522][    C6]  handle_bad_stack+0x34/0x50
[  282.335534][    C6]  __bad_stack+0x70/0x94
[  282.335544][    C6]  sched_clock+0x8/0x60
[  282.335556][    C6]  vprintk_emit+0x8c/0x13c
[  282.335567][    C6]  vprintk_default+0x48/0x74
[  282.335582][    C6]  vprintk+0xf8/0x13c
[  282.335595][    C6]  _printk+0x58/0x84
[  282.335608][    C6]  recursive_loop+0xac/0xac [lkdtm]
[  282.335639][    C6]  recursive_loop+0x78/0xac [lkdtm]
[  282.335656][    C6]  recursive_loop+0x78/0xac [lkdtm]
[  282.335697][    C6]  recursive_loop+0x78/0xac [lkdtm]
[  282.335687][    C6]  recursive_loop+0x78/0xac [lkdtm]
[  282.335705][    C6]  recursive_loop+0x78/0xac [lkdtm]
[  282.335721][    C6]  recursive_loop+0x78/0xac [lkdtm]
[  282.335737][    C6]  recursive_loop+0x78/0xac [lkdtm]
[  282.335753][    C6]  recursive_loop+0x78/0xac [lkdtm]
[  282.335769][    C6]  recursive_loop+0x78/0xac [lkdtm]
[  282.335785][    C6]  recursive_loop+0x78/0xac [lkdtm]
[  282.335800][    C6]  recursive_loop+0x78/0xac [lkdtm]
[  282.335814][    C6]  recursive_loop+0x78/0xac [lkdtm]
[  282.335829][    C6]  lkdtm_EXHAUST_STACK+0x34/0x54 [lkdtm]
[  282.335845][    C6]  lkdtm_do_action+0x30/0x38 [lkdtm]
[  282.335859][    C6]  init_module+0c130/0x274 [lkdtm]
[  282.335870][    C6]  do_one_initcall+0x48/0x208
[  282.335880][    C6]  do_init_module+0x6c/0x264
[  282.335895][    C6]  load_module+0x1968/0x1c0
[  282.335906][    C6]  __arm64_sys_finit_module+0xbc/0xfc
[  282.335918][    C6]  invoke_syscall+0x44/0x120
[  282.335918][    C6]  el0_svc_common+0x88/0xf8
[  282.335927][    C6]  do_el0_svc+0x28/0x88
[  282.335936][    C6]  el0_svc+0x24/0x84
[  282.335945][    C6]  el0t_64_sync_handler+0x88/0xec
[  282.335950][    C6]  el0t_64_sync+0x1b4/0x1b8
[  282.335957][    C6] SMP: stopping secondary CPUs
[  282.336010][    C1] debug-snapshot dss: core register saved(CPU:1)
[  282.336261][    C1] debug-snapshot dss: context saved(CPU:1)
```

CRASHTYPE(CORRUPT_STACK) => ramdump.

and_CORRUPT_STACK_log.txt

```
:console:/ # rmmod lkdtn.ko
r_dlkm/lib/modules/lkdtn.ko cpoint_name=DIRECT cpoint_type=CORRUPT_STACK      <
[  104.964177][ T4017] Kernel panic - not syncing: stack-protector: Kernel stack is corrupted in: lkdtn_CORRUPT_STACK+0x60/0x60 [lkdtn]
[  104.966032][ T4017] CPU: 6 PID: 4017 Comm: insmod Tainted: G            E     5.15.41-android13-8-gd18b75b8b12b #1
[  104.967694][ T4017] Hardware name: BMW IDCEvo (SP21-v920-B1) Android IVI VM (DT)
[  104.969098][ T4017] Call trace:
[  104.969216][ T4017]  dump_backtrace+0x0/0x1d4
[  104.969410][ T4017]  show_stack+0x1c/0x2c
[  104.970593][ T4017]  dump_stack_lvl+0x68/0x84
[  104.970779][ T4017]  dump_stack+0x1c/0x40
[  104.970946][ T4017]  panic+0x164/0x3a8
[  104.972225][ T4017]  rcu_dynticks_inc+0x0/0x64
[  104.992275][ T4017]  __lkdtn_CORRUPT_STACK+0x0/0x20 [lkdtn]
[  104.992518][ T4017]  0xffffffffffffffff
[  104.993709][ T4017] SMP: stopping secondary CPUs
[  104.993940][    C1] debug-snapshot dss: core register saved(CPU:1)
[  104.995373][    C1] debug-snapshot dss: context saved(CPU:1)
[  105.015469][    C1] CPU: 1 PID: 0 Comm: swapper/1 Tainted: G            E     5.15.41-android13-8-gd18b75b8b12b #1
[  105.017024][    C1] Hardware name: BMW IDCEvo (SP21-v920-B1) Android IVI VM (DT)
[  105.017353][    C1] Call trace:
[  105.037346][    C1]  dump_backtrace+0x0/0x1d4
[  105.037610][    C1]  show_stack+0x1c/0x2c
[  105.037778][    C1]  dump_stack_lvl+0x68/0x84
[  105.039054][    C1]  dump_stack+0x1c/0x40
[  105.039227][    C1]  dbg_snapshot_save_context+0x2b0/0x2bc [dss]
[  105.059273][    C1]  dbg_snapshot_ipi_stop+0x28/0x38 [dss]
[  105.059584][    C1]  __traceiter_android_vh_ipi_stop+0x34/0x54
[  105.060865][    C1]  do_handle_IPI+0x184/0x1a4
[  105.061068][    C1]  ipi_handler+0x20/0x34
[  105.081056][    C1]  handle_percpu_devid_irq+0x88/0x21c
[  105.081297][    C1]  handle_domain_irq+0x60/0xa8
[  105.082521][    C1]  gic_handle_irq+0x54/0x12c
[  105.082720][    C1]  call_on_irq_stack+0x40/0x70
[  105.082917][    C1]  do_interrupt_handler+0x40/0x58
[  105.102949][    C1]  el1_interrupt+0x34/0x60
[  105.103145][    C1]  el1h_64_irq_handler+0x1c/0x2c
[  105.104373][    C1]  el1h_64_irq+0x7c/0x80
[  105.104550][    C1]  arch_local_irq_enable+0xc/0x18
[  105.104759][    C1]  default_idle_call+0x3c/0x14c
[  105.124794][    C1]  do_idle+0x100/0x298
[  105.124983][    C1]  cpu_startup_entry+0x28/0x2c
[  105.126214][    C1]  secondary_start_kernel+0x194/0x1cc
[  105.126434][    C1]  __secondary_switched+0x98/0x9c
[  105.146597][    C2] debug-snapshot dss: core register saved(CPU:2)
```

CRASHTYPE(WRITE_AFTER_FREE), => no restart

and_write_after_free_log.txt

```
1console:/ # rmmod lkdtn.ko
tn.ko cpoint_name=DIRECT cpoint_type=WRITE_AFTER_FREE                      <
console:/ # [  133.014956][ T4488] Unable to handle kernel paging request at virtual address 0023438289000 1ff
[  133.016641][ T4488] Mem abort info:
[  133.016881][ T4488]   ESR = 0x96000004
[  133.017130][ T4488]   EC = 0x25: DABT (current EL), IL = 32 bits
[  133.018768][ T4488]   SET = 0, FnV = 0
[  133.019033][ T4488]   EA = 0, S1PTW = 0
[  133.019194][ T4488]   FSC = 0x04: level 0 translation fault
[  133.020435][ T4488] Data abort info:
[  133.020585][ T4488]   ISV = 0, ISS = 0x00000004
[  133.021979][ T4488]   CM = 0, WnR = 0
[  133.022181][ T4488] [0023438289000 1ff] address between user and kernel address ranges
[  133.023507][ T4488] Internal error: Oops: 96000004 [#1] PREEMPT SMP
[  133.043705][ T4488] debug-snapshot dss: core register saved(CPU:6)
[  133.043959][ T4488] debug-snapshot dss: context saved(CPU:6)
[  133.045219][ T4488] item - log_kevents is disabled
[  133.045410][ T4488]
[  133.045410][ T4488] PC:
```

CRASHTYPE(READ_AFTER_FREE),=> no crash

and_read_after_free_log.txt

```
console:/ # rmmod lkdtm.ko
r_dlkm/lib/modules/lkdtm.ko cpoint_name=DIRECT cpoint_type=READ_AFTER_FREE    <
console:/ #
console:/ #
console:/ #
console:/ #
```

CRASHTYPE(HUNG_TASK), => just hang,no reboot.on restart, no ram dump.

and_HUNG_TASK_log.txt

```
console:/ # rmmod lkdtm.ko
r_dlkm/lib/modules/lkdtm.ko cpoint_name=DIRECT cpoint_type=HUNG_TASK          <



^C
^Z
```

CRASHTYPE(EXEC_KMALLOC) => just dss, no reboot. no ramdump

and_EXEC_KMALLOC_log.txt

```
console:/ # rmmod lkdtm.ko
r_dlkm/lib/modules/lkdtm.ko cpoint_name=DIRECT cpoint_type=EXEC_KMALLOC        <
[   98.502148][ T3938] Unable to handle kernel execute from non-executable memory at virtual address ffffff8810ad1800
[   98.504027][ T3938] Mem abort info:
[   98.505283][ T3938]   ESR = 0x86000000f
[   98.505545][ T3938]   EC = 0x21: IABT (current EL), IL = 32 bits
[   98.507035][ T3938]   SET = 0, FnV = 0
[   98.507274][ T3938]   EA = 0, S1PTW = 0
[   98.507434][ T3938]   FSC = 0x0f: level 3 permission fault
[   98.508678][ T3938] swapper pgtable: 4k pages, 39-bit VAs, pgdp=00000000b21aa000
[   98.508969][ T3938] [ffffff8810ad1800] pgd=1800000a7fdc2003, p4d=1800000a7fdc2003, pud=1800000a7fdc2003, pmd=1800000a7fd3c003, pte=0068000890ad1707
[   98.511997][ T3938] Internal error: Oops: 86000000f [#1] PREEMPT SMP
[   98.531871][ T3938] debug-snapshot dss: core register saved(CPU:5)
[   98.532142][ T3938] debug-snapshot dss: context saved(CPU:5)
[   98.533370][ T3938] item - log_kevents is disabled
```

CRASHTYPE(EXEC_VMALLOC) => ramdump

and_EXEC_VMALLOC_log.txt

```
console:/ # rmmod lkdtm.ko
r_dlkm/lib/modules/lkdtm.ko cpoint_name=DIRECT cpoint_type=EXEC_VMALLOC       <
[  108.571801][ T4033] Unable to handle kernel execute from non-executable memory at virtual address ffffffc00d2e5000
[  108.572574][ T4033] Mem abort info:
[  108.573485][ T4033]   ESR = 0x8600000f
[  108.573735][ T4033]   EC = 0x21: IABT (current EL), IL = 32 bits
[  108.575589][ T4033]   SET = 0, FnV = 0
[  108.575959][ T4033]   EA = 0, S1PTW = 0
[  108.576117][ T4033]   FSC = 0x0f: level 3 permission fault
[  108.577417][ T4033] swapper pgtable: 4k pages, 39-bit VAs, pgdp=00000000b21aa000
[  108.579077][ T4033] [ffffffc00d2e5000] pgd=1000000a7ffff003, p4d=1000000a7ffff003, pud=1000000a7ffff003, pmd=100000088c10b003, pte=006800095d20b703
[  108.580687][ T4033] Internal error: Oops: 8600000f [#1] PREEMPT SMP
[  108.594526][    T1] init: starting service 'vendor.gatekeeper-1-0'...
[  108.600935][ T4033] debug-snapshot dss: core register saved(CPU:6)
[  108.602412][ T4033] debug-snapshot dss: context saved(CPU:6)
[  108.603346][    T1] init: Control message: Processed ctl.interface_start for 'android.hardware.gatekeeper@1.0::IGatekeeper/default' from pid: 291 (/system/bin/hwservicemanager)
[  108.622518][ T4033] item - log_kevents is disabled
[  108.622552][ T4033]
```

CRASHTYPE(USERCOPY_KERNEL) => ramdump

and_USERCOPY_KERNEL_log.txt

```
console:/ # rmmod lkdtm.ko
tm.ko cpoint_name=DIRECT cpoint_type=USERCOPY_KERNEL                    <
   99.619520][ T3920] usercopy: Kernel memory exposure attempt detected from kernel text (offset 2834560, size 4096)!
   99.621480][ T3920] kernel BUG at mm/usercopy.c:99!
   99.621831][ T3920] Internal error: Oops - BUG: 0 [#1] PREEMPT SMP
   99.623399][ T3920] debug-snapshot dss: core register saved(CPU:3)
   99.623762][ T3920] debug-snapshot dss: context saved(CPU:3)
   99.624121][   T300] logd: logd: UID=1000 GID=1000 PID=3915 n tail=0 logMask=8 pid=3912 start=0ns deadline=0ns
   99.624197][    T1] init: SVC_EXEC service 'exec 105 (/system/bin/flags_health_check UPDATABLE_CRASHING)' pid 3921 (uid 1000 gid 1000+0 context default) started; waiting...
   99.625021][ T3920] item - log_kevents is disabled
```

Release	ES2
HW	SP25
SYS	

Soft Lockup :

The Linux kernel can act as a watchdog to detect both soft and hard lockups.

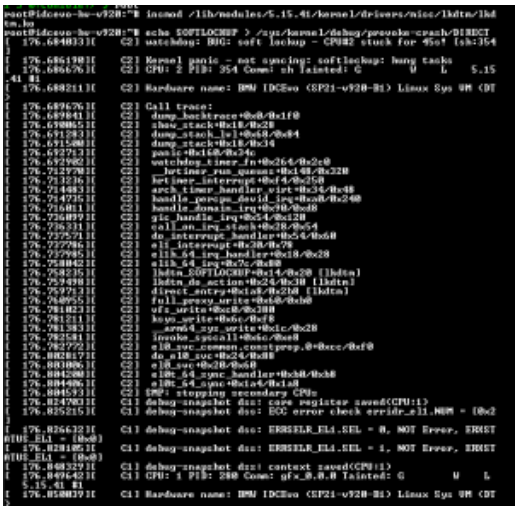
A ‘softlockup’ is defined as a bug that causes the kernel to loop in kernel mode for more than 20 seconds without giving other tasks a chance to run.

Soft lockup is triggered with Linux kernel Dump Test Module(LKDTM).

soft lockup is triggered by below commands.

```
# insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkdtm.ko
# echo SOFTLOCKUP > /sys/kernel/debug/provoke-crash/DIRECT
```

Call stack



```
root@idcevo-hw-v920:~# insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkd
tm.ko
root@idcevo-hw-v920:~# echo SOFTLOCKUP > /sys/kernel/debug/provoke-crash/DIRECT
[  176.684833][    C2] watchdog: BUG: soft lockup - CPU#2 stuck for 45s! [sh:354
]
[  176.686190][    C2] Kernel panic - not syncing: softlockup: hung tasks
[  176.686676][    C2] CPU: 2 PID: 354 Comm: sh Tainted: G        W   L    5.15
.41 #1
[  176.688211][    C2] Hardware name: BMW IDCEvo (SP21-v920-B1) Linux Sys UM (DT
)
[  176.689676][    C2] Call trace:
[  176.689841][    C2]  dump_backtrace+0x0/0x1f0
[  176.690065][    C2]  show_stack+0x18/0x28
[  176.691383][    C2]  dump_stack_lvl+0x68/0x84
[  176.691580][    C2]  dump_stack+0x18/0x34
[  176.692713][    C2]  panic+0x168/0x34c
[  176.692902][    C2]  watchdog_timer_fn+0x264/0x2c0
[  176.712978][    C2]  __hrtimer_run_queues+0x148/0x320
[  176.713236][    C2]  hrtimer_interrupt+0xf4/0x250
[  176.714883][    C2]  arch_timer_handler_virt+0x34/0x48
[  176.714735][    C2]  handle_percpu_devid_irq+0xa8/0x240
[  176.716011][    C2]  handle_domain_irq+0x90/0xd8
[  176.716899][    C2]  gic_handle_irq+0x54/0x120
[  176.736331][    C2]  call_on_irq_stack+0x28/0x54
[  176.737571][    C2]  do_interrupt_handler+0x54/0x60
[  176.737786][    C2]  el1_interrupt+0x38/0x70
[  176.737985][    C2]  el1h_64_irq_handler+0x18/0x28
[  176.738042][    C2]  el1h_64_irq+0x7c/0x80
[  176.758235][    C2]  lkdtm_SOFTLOCKUP+0x14/0x20 [lkdtm]
[  176.759498][    C2]  lkdtm_do_action+0x24/0x38 [lkdtm]
[  176.759713][    C2]  direct_entry+0x1a8/0x230 [lkdtm]
[  176.760955][    C2]  full_proxy_write+0x68/0xb0
[  176.781823][    C2]  vfs_write+0xc8/0x3f0
[  176.781211][    C2]  ksys_write+0x6c/0xf0
[  176.781383][    C2]  __arm64_sys_write+0x1c/0x20
[  176.782581][    C2]  invoke_syscall+0x6c/0xe0
[  176.782792][    C2]  el0_svc_common.constprop.0+0xcc/0xf0
[  176.882817][    C2]  do_el0_svc+0x24/0x88
[  176.883086][    C2]  el0_svc+0x20/0x60
[  176.884208][    C2]  el0t_64_sync_handler+0xb8/0xb0
[  176.884086][    C2]  el0t_64_sync+0x1a4/0x1a8
[  176.884593][    C2] SMP: stopping secondary CPUs
[  176.824703][    C1] debug-snapshot dss: core register saved(CPU:1)
[  176.825215][    C1] debug-snapshot dss: ECC error check error.s11.MEM = [0x2
]
[  176.826632][    C1] debug-snapshot dss: ERRSELR_EL1.SEL = 0, NOT Error, ERRST
ATUS_EL1 = [0x0]
[  176.828185][    C1] debug-snapshot dss: ERRSELR_EL1.SEL = 1, NOT Error, ERRST
ATUS_EL1 = [0x0]
[  176.848329][    C1] debug-snapshot dss: context saved(CPU:1)
[  176.849642][    C1] CPU: 1 PID: 280 Comm: gfx_0.0.0 Tainted: G        W   L
    5.15.41 #1
[  176.850839][    C1] Hardware name: BMW IDCEvo (SP21-v920-B1) Linux Sys UM (DT
)
```

Soft lockup logs

softlockup_log_sys_es2.txt

Ramdump kernel sys logs

soflockup_kernel_sys_es2.lst

Hard Lockup :

A ‘hardlockup’ is defined as a bug that causes the CPU to loop in kernel mode for more than 10 seconds, without letting other interrupts have a chance to run.

Hard lockup is triggered with Linux kernel Dump Test Module(LKDTM).

Below are the steps to trigger hard LOCKUP

```
# insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkdtm.ko
# echo HARDLOCKUP > /sys/kernel/debug/provoke-crash/DIRECT
```

Call Stack

Hardlockup logs

hardlockup_log_sys_es2.txt

Ramdump kernel logs

hardlockup_kernel_sys_es2.lst

Hung_Task:

The hung task is detected by linux kernel by parsing processes with uninterruptible sleep state(which are waiting for some event or resource and is usually not going to move forward) for long time and which are stalled into this D state.

```
echo HUNG_TASK > /sys/kernel/debug/provoke-crash/DIRECT
```

root@idcevo-hv-v920:~# zcat /proc/config.gz | grep HUNG_TASK
CONFIG_DETECT_HUNG_TASK=y
CONFIG_DEFAULT_HUNG_TASK_TIMEOUT=120
CONFIG_BOOTPARAM_HUNG_TASK_PANIC=y
CONFIG_BOOTPARAM_HUNG_TASK_PANIC_VALUE=1

hung_task_panic_value If set to 1, the kernel panics if any user or kernel thread sleeps in the TASK_UNINTERRUPTIBLE state (D state) for more than HUNG_TASK_TIMEOUT seconds. A process remains in D state while waiting for I/O to complete. You cannot kill or interrupt a process in this state.

Call Stack

```
root@idcevo-hv-v920:~# zcat /proc/config.gz | grep HUNG_TASK
zcat: /: No such file or directory
CONFIG_DETECT_HUNG_TASK=y
CONFIG_DEFAULT_HUNG_TASK_TIMEOUT=120
CONFIG_BOOTPARAM_HUNG_TASK_PANIC=y
CONFIG_BOOTPARAM_HUNG_TASK_PANIC_VALUE=1
root@idcevo-hv-v920:~# echo HUNG_TASK > /sys/kernel/debug/provoke-crash/DIRECT
-sh: /sys/kernel/debug/provoke-crash/DIRECT: No such file or directory
root@idcevo-hv-v920:~# insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkdtm.ko
root@idcevo-hv-v920:~# echo HUNG_TASK > /sys/kernel/debug/provoke-crash/DIRECT
[  242.665357][   T31] INFO: task sh:352 blocked for more than 120 seconds.
[  242.668741][   T31]       Tainted: G           O      5.15.41 #1
[  242.670277][   T31] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.
[  242.674947][   T31] task:sh              state:D stack:    0 pid:  352 ppid:     1 flags:0x00000200
[  242.675731][   T31] Call trace:
[  242.676985][   T31]  __switch_to+0x10c/0x1c8
[  242.677269][   T31]  __schedule+0x8bc/0x1338
[  242.677537][   T31]  schedule+0x44/0xf8
[  242.683981][   T31]  lkdtm_HUNG_TASK+0x2c/0x38 [lkdtm]
[  242.684490][   T31]  lkdtm_do_action+0x24/0x30 [lkdtm]
[  242.685795][   T31]  direct_entry+0x1a8/0x2b8 [lkdtm]
[  242.686954][   T31]  full_proxy_write+0x60/0xb0
[  242.688385][   T31]  vfs_write+0xc0/0x380
[  242.688661][   T31]  ksys_write+0x6c/0xf8
[  242.710007][   T31]  __arm64_sys_write+0x1c/0x28
[  242.710317][   T31]  invoke_syscall+0x6c/0xe8
[  242.713895][   T31]  el0_svc_common.constprop.0+0xcc/0xf0
[  242.715568][   T31]  do_el0_svc+0x24/0x88
[  242.715987][   T31]  el0_svc+0x20/0x60
[  242.717972][   T31]  el0t_64_sync_handler+0xb0/0xb8
[  242.720474][   T31]  el0t_64_sync+0x1a4/0x1a8
[  242.740397][   T31] Kernel panic - not syncing: hung_task: blocked tasks
[  242.740925][   T31] CPU: 0 PID: 31 Comm: khungtaskd Tainted: G           O      5.15.41 #1
[  242.742466][   T31] Hardware name: BMW IDCEvo (SP21-v920-B1) Linux Sys VM (DT)
[  242.743978][   T31] Call trace:
[  242.763907][   T31]  dump_backtrace+0x0/0x1f0
[  242.764151][   T31]  show_stack+0x10/0x20
[  242.764360][   T31]  dump_stack_lvl+0x68/0x84
[  242.765653][   T31]  dump_stack+0x18/0x34
[  242.765875][   T31]  panic+0x160/0x34c
[  242.785874][   T31]  watchdog+0x2ec/0x500
[  242.786094][   T31]  kthread+0x144/0x158
[  242.786298][   T31]  ret_from_fork+0x10/0x20
[  242.787543][   T31] SMP: stopping secondary CPUs
[  242.787830][    C1] debug-snapshot dss: core register saved(CPU:1)
[  242.807933][    C1] debug-snapshot dss: ECC error check erridr_el1.NUM = [0x2]
[  242.809382][    C1] debug-snapshot dss: ERRSELR_EL1.SEL = 0, NOT Error, ERRSTATUS_EL1 = [0x0]
[  242.809849][    C1] debug-snapshot dss: ERRSELR_EL1.SEL = 1, NOT Error, ERRSTATUS_EL1 = [0x0]
[  242.811323][    C1] debug-snapshot dss: context saved(CPU:1)
```

Hung task logs

hung_task_es2_sys_log.txt

Ramdump kernel logs

hungtask_kernel_sys_es2.lst

LKDTM testing

SYS side

Tried crash-> ramdump with latest ES2.sys files built, on top of COCKPIT_ARTIFACTS_234.

tried with the command, "insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkdtm.ko cpoint_name=DIRECT cpoint_type=<*CRASHTYPE*>"

CRASHTYPE(BUG) => ramdump is generated.

```
root@idcevo-hw-v920:~# insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkdtm.ko cpoint_name=DIRECT cpoint_type=BUG
[  318.514752][ T6204] kernel BUG at drivers/misc/lkdtm/bugs.c:76!
[  318.515304][ T6204] Internal error: Oops - BUG: 0 [#1] PREEMPT SMP
[  318.516876][ T6204] debug-snapshot dss: core register saved(CPU:2)
[  318.517330][ T6204] debug-snapshot dss: ECC error check errridr_el1.NUM = [0x2]
[  318.518851][ T6204] debug-snapshot dss: ERRSELR_EL1.SEL = 0, NOT Error, ERXSTATUS_EL1 = [0x0]
[  318.520291][ T6204] debug-snapshot dss: ERRSELR_EL1.SEL = 1, NOT Error, ERXSTATUS_EL1 = [0x0]
[  318.521712][ T6204] debug-snapshot dss: context saved(CPU:2)
[  318.521989][ T6204] item - log_kevents is disabled
[  318.523243][ T6204]
[  318.523243][ T6204] PC:
[  318.543305][ T6204] b378 : ******** ******** ******** ******** ******** ******** ******** ********
[  318.544758][ T6204] b398 : ******** ******** ******** ******** ******** ******** ******** ********
[  318.545170][ T6204] b3b8 : ******** ******** ******** ******** ******** ******** ******** ********
[  318.565378][ T6204] b3d8 : ******** ******** ******** ******** ******** ******** ******** ********
[  318.566820][ T6204] b3f8 : ******** ******** ******** ******** ******** ******** ******** ********
[  318.568226][ T6204] b418 : ******** ******** ******** ******** ******** ******** ******** ********
[  318.572724][    C0] [ IPC:process_uframe_timeo: 672 ] [ERR] 0: 'uframe_timer/0' timeout
[  318.588462][ T6204] b438 : ******** ******** ******** ******** ******** ******** ******** ********
[  318.591466][ T6204] b458 : ******** ******** ******** ******** ******** ******** ******** ********
[  318.611693][ T6204]
[  318.611693][ T6204] LR:
[  318.612948][ T6204] d5f8 : ******** ******** ******** ******** ******** ******** ******** ********
[  318.613392][ T6204] d618 : ******** ******** ******** ******** ******** ******** ******** ********
[  318.633634][ T6204] d638 : ******** ******** ******** ******** ******** ******** ******** ********
[  318.635139][ T6204] d658 : ******** ******** ******** ******** ******** ******** ******** ********
[  318.655315][ T6204] d678 : ******** ******** ******** ******** ******** ******** ******** ********
```

crashtype bug logs

sys_es2_bug_log.txt

ramdump kernel logs

bug_kernel_sys_es2.lst

CRASHTYPE(EXCEPTION) => ramdump is generated.

```
root@idcevo-hv-v920:~# insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkdtm.ko cpoint_name=DIRECT cpoint_type=EXCEPTION
[  115.202222][ T6629] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000
[  115.204523][ T6629] Mem abort info:
[  115.205118][ T6629]   ESR = 0x96000045
[  115.206677][ T6629]   EC = 0x25: DABT (current EL), IL = 32 bits
[  115.209117][ T6629]   SET = 0, FnV = 0
[  115.210508][ T6629]   EA = 0, S1PTW = 0
[  115.210857][ T6629]   FSC = 0x05: level 1 translation fault
[  115.212504][ T6629] Data abort info:
[  115.214144][ T6629]   ISV = 0, ISS = 0x00000045
[  115.214413][ T6629]   CM = 0, WnR = 1
[  115.214600][ T6629] user pgtable: 4k pages, 39-bit VAs, pgdp=0000000ab57ab000
[  115.217984][ T6629] [0000000000000000] pgd=0000000000000000, p4d=0000000000000000, pud=0000000000000000
[  115.220171][ T6629] Internal error: Oops: 96000045 [#1] PREEMPT SMP
[  115.240027][ T6629] debug-snapshot dss: core register saved(CPU:1)
[  115.240374][ T6629] debug-snapshot dss: ECC error check erridr_el1.NUM = [0x2]
[  115.241749][ T6629] debug-snapshot dss: ERRSELR_EL1.SEL = 0, NOT Error, ERXSTATUS_EL1 = [0x0]
EL1.SEL = 1, NOT Error, ERXSTATUS_EL1 = [0x0]RSELR_
[  115.263699][ T6629] debug-s
napshot dss: conteBroxt sadcavast med(essaCPU:1)
[  115.265719][ T6629] item - log_kevents is disabled
g[ e fro 1m 15sy.2st85em80d-j3][ T6our62nal9]d@i
[dc  ev115.28o-hv-58v90320][ (Sat  T6229] PC:
022-01-[ 01 12: 101:15.254 UT8828C):
```

teraterm logs

sys_es2_exception_log.txt

Ramdump logs

exception_kernel_sys_es2.lst

CRASHTYPE(EXHAUST_STACK) =>ramdump

```
root@idcevo-hv-v920:~# insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkdtm.ko cpoint_name=DIRECT cpoint_type=EXHAUST_STACK
0 HYP:[+104714 ms] [00108908 ms] System-wide panic initiated from VM2.
[  101.295143][    C0] Kernel panic - not syncing: System wide panic initiated.
1 3 0:[  101.295654][    C0] CPU: 0 PID: 0 Comm: swapper/0 Tainted: G        V   E     5.15.41-android13-8-ga7d17ad643ca #1
1 3 0:[  101.297206][    C0] Hardware name: BMW IDCEvo (SP21-v920-B1) Android IVI VM (DT)
1 3 0:[  101.298576][    C0] Call trace:
1 3 0:[  101.298660][    C0]  dump_backtrace+0x0/0x208
1 3 0:[  101.298796][    C0]  show_stack+0x1c/0x2c
1 3 0:[  101.299907][    C0]  dump_stack_lvl+0x68/0x84
1 3 0:[  101.300037][    C0]  dump_stack+0x1c/0x40
1 3 0:[  101.301167][    C0]  panic+0x164/0x3a8
1 3 0:[  101.301268][    C0]  _panic_trigger_sysconf+0xc0/0xf80 [vlx_panic_trigger_module]
6 3 4:[  101.305128][    T1] init: starting service 'vendor.gatekeeper-1-0'...
1 3 0:[  101.321304][    C0]  nk_xirq_handler+0x1c/0x30
1 3 0:[  101.321329][    C0]  __handle_irq_event_percpu+0x88/0x220
```

teraterm logs

sys_es2_EXHAUST_STACK_log.txt

ramdump logs

exhaust_stack_kernel_sys_es2.lst

CRASHTYPE(CORRUPT_STACK) =>ramdump

```
root@idcevo-hw-v920:~# insmod /lib/modules/5.15.41/kernel/drivers/misc/lkdtm/lkdtm.ko cpoint_name=DIRECT cpoint_type=CORRUPT_STACK
[  164.581132][T10294] Kernel panic - not syncing: stack-protector: Kernel stack is corrupted in: lkdtm_CORRUPT_STACK+0x48/0x58 [lkdtm]
[  164.583152][T10294] CPU: 1 PID: 10294 Comm: insmod Tainted: G        W          5.15.41 #1
[  164.584809][T10294] Hardware name: BMW IDCEvo (SP21-v920-B1) Linux Sys VM (DT)
[  164.585291][T10294] Call trace:
[  164.586492][T10294]  dump_backtrace+0x0/0x1f0
[  164.586736][T10294]  show_stack+0x18/0x28
[  164.586938][T10294]  dump_stack_lvl+0x68/0x84
[  164.588210][T10294]  dump_stack+0x18/0x34
[  164.588436][T10294]  panic+0x160/0x34c
[  164.588646][T10294]  __stack_chk_fail+0x30/0x40
[  164.608713][T10294]  lkdtm_CORRUPT_STACK+0x48/0x58 [lkdtm]
[  164.608994][T10294]  lkdtm_do_action+0x24/0x30 [lkdtm]
[  164.610271][T10294]  0xffffffffffffffff
```

teraterm logs

sys_es2_corrupt_stack_log.txt

ramdump logs

corrupt_stack_kernel_sys_es2.lst

CRASHTYPE(WRITE_AFTER_FREE), => no crash

CRASHTYPE(READ_AFTER_FREE),=> no crash

CRASHTYPE(EXEC_KMALLOC) => ramdump
CRASHTYPE(EXEC_VMALLOC) => ramdump
CRASHTYPE(USERCOPY_KERNEL) => ramdump
CRASHTYPE(HUNG_TASK) => ramdump

Release	ES2
HW	SP25
IVI	

Following commands for lkdtm on android.

console:/ # rmmod lkdtm.ko
console:/ # insmod /vendor_dlkm/lib/modules/lkdtm.ko cpoint_name=DIRECT cpoint_type=HUNG_TASK

CRASHTYPE(HARDLOCKUP) => ramdump is generated.

```
s/lkdtm.ko cpoint_name=DIRECT cpoint_type=HARDLOCKUP                                <
[  689.750299][    C0] Kernel panic - not syncing: Watchdog detected hard LOCKUP on cpu 1
[  689.751906][    C0] CPU: 0 PID: 0 Comm: swapper/0 Tainted: G        W   E     5.15.41-android13-8-ga7d17ad643ca #1
[  689.753582][    C0] Hardware name: BMW IDCEvo (SP21-v920-B1) Android IVI VM (DT)
[  689.755071][    C0] Call trace:
[  689.755204][    C0]  dump_backtrace+0x0/0x208
[  689.755406][    C0]  show_stack+0x1c/0x2c
[  689.756605][    C0]  dump_stack_lvl+0x68/0x84
[  689.756857][    C0]  dump_stack+0x1c/0x40
[  689.757036][    C0]  panic+0x164/0x3a8
[  689.758286][    C0]  hardlockup_stop_fn+0x0/0xe0 [hardlockup_watchdog]
[  689.758574][    C0]  __run_hrtimer+0xa8/0x26c
[  689.778572][    C0]  hrtimer_interrupt+0x1e4/0x2cc
[  689.778786][    C0]  arch_timer_handler_virt+0x40/0x54
[  689.780038][    C0]  handle_percpu_devid_irq+0x88/0x21c
[  689.780275][    C0]  handle_domain_irq+0x60/0xa8
[  689.800273][    C0]  gic_handle_irq+0x54/0x12c
[  689.800487][    C0]  call_on_irq_stack+0x40/0x70
[  689.801739][    C0]  do_interrupt_handler+0x40/0x58
[  689.801948][    C0]  el1_interrupt+0x34/0x60
[  689.802130][    C0]  el1h_64_irq_handler+0x1c/0x2c
[  689.822143][    C0]  el1h_64_irq+0x7c/0x80
[  689.822335][    C0]  arch_local_irq_enable+0xc/0x18
[  689.823584][    C0]  default_idle_call+0x3c/0x14c
[  689.823813][    C0]  do_idle+0x100/0x298
[  689.824014][    C0]  cpu_startup_entry+0x28/0x2c
[  689.844111][    C0]  rest_init+0xe4/0xf8
[  689.844320][    C0]  arch_call_rest_init+0x14/0x24
[  689.845561][    C0]  start_kernel+0x37c/0x494
[  689.845781][    C0]  __primary_switched+0xc4/0xcc
```

CRASHTYPE(SOFTLOCKUP) => hanging

```
r_dlkm/lib/modules/lkdtm.ko cpoint_name=DIRECT cpoint_type=SOFTLOCKUP          <
[    92.036596][    C5] watchdog: BUG: soft lockup - CPU#5 stuck for 44s! [insmod:1802]
[   116.036595][    C5] watchdog: BUG: soft lockup - CPU#5 stuck for 67s! [insmod:1802]
[   123.896656][    C0] BUG: workqueue lockup - pool cpus=5 node=0 flags=0x0 nice=0 stuck for 78s!
[   156.036591][    C5] watchdog: BUG: soft lockup - CPU#5 stuck for 104s! [insmod:1802]
[   180.036598][    C5] watchdog: BUG: soft lockup - CPU#5 stuck for 126s! [insmod:1802]
[   185.336662][    C0] BUG: workqueue lockup - pool cpus=5 node=0 flags=0x0 nice=0 stuck for 140s!
[   220.036597][    C5] watchdog: BUG: soft lockup - CPU#5 stuck for 163s! [insmod:1802]
[   244.036595][    C5] watchdog: BUG: soft lockup - CPU#5 stuck for 186s! [insmod:1802]
[   246.764645][    C0] BUG: workqueue lockup - pool cpus=5 node=0 flags=0x0 nice=0 stuck for 201s!
```

CRASHTYPE(HUNG_TASK) => hanging

CRASHTYPE(PANIC) => ramdump is generated.

CRASHTYPE(BUG) => ramdump is generated.

CRASHTYPE(EXCEPTION) => ramdump is generated.

CRASHTYPE(EXHAUST_STACK) =>ramdump generated

CRASHTYPE(CORRUPT_STACK) =>ramdump generated

CRASHTYPE(WRITE_AFTER_FREE) => ramdump

```
console:/ $ su
console:/ # rmmod lkdtm.ko
r_dlkm/lib/modules/lkdtm.ko cpoint_name=DIRECT cpoint_type=WRITE_AFTER_FREE   <
console:/ # [   63.001166][ T2654] Unable to handle kernel paging request at virtual address 005a22eea78c9c8d
[   63.002255][ T2654] Mem abort info:
[   63.003140][ T2654]   ESR = 0x96000004
[   63.003439][ T2654]   EC = 0x25: DABT (current EL), IL = 32 bits
[   63.004845][ T2654]   SET = 0, FnV = 0
[   63.005094][ T2654]   EA = 0, S1PTW = 0
[   63.005264][ T2654]   FSC = 0x04: level 0 translation fault
[   63.006819][ T2654] Data abort info:
[   63.007129][ T2654]   ISV = 0, ISS = 0x00000004
[   63.008448][ T2654]   CM = 0, WnR = 0
[   63.008694][ T2654] [005a22eea78c9c8d] address between user and kernel address ranges
[   63.010173][ T2654] Internal error: Oops: 96000004 [#1] PREEMPT SMP
[   63.030480][ T2654] debug-snapshot dss: core register saved(CPU:1)
[   63.030768][ T2654] debug-snapshot dss: context saved(CPU:1)
[   63.031994][ T2654] item - log_kevents is disabled
[   63.032182][ T2654]
[   63.032182][ T2654] PC:
[   63.040877][    T1] init: starting service 'watchdogd'...
[   63.052187][ T2654] 9008 : ******** ******** ******** ******** ******** ******** ******** ********
[   63.052243][ T2654] 9028 : ******** ******** ******** ******** ******** ******** ******** ********
[   63.052271][ T2654] 9048 : ******** ******** ******** ******** ******** ******** ******** ********
[   63.052299][ T2654] 9068 : ******** ******** ******** ******** ******** ******** ******** ********
[   63.052326][ T2654] 9088 : ******** ******** ******** ******** ******** ******** ******** ********
[   63.052357][ T2654] 90a8 : ******** ******** ******** ******** ******** ******** ******** ********
[   63.052393][ T2654] 90c8 : ******** ******** ******** ******** ******** ******** ******** ********
```

CRASHTYPE(READ_AFTER_FREE),=> no error

```
1!console:/ # rmmod lkdtm.ko
dtm.ko cpoint_name=DIRECT cpoint_type=READ_AFTER_FREE
console:/ #
```

CRASHTYPE(EXEC_KMALLOC) => ramdump
CRASHTYPE(EXEC_VMALLOC) => ramdump
CRASHTYPE(USERCOPY_KERNEL) => ramdump

Steps to trigger Manual Ram Dump

1. Send a command via INC channel 12 to enable manual ram dump
   echo -e -n '\x01\x00\x00\x10\x00\x**00**' > /dev/ipc12 - Enables manual ram dump across sleep cycles (Persisted across sleep cycle - stored in retention ram, not persisted across battery cycle)
   Look for MCU DLT Trace - **[BCP] set RTN RAM manual RAM dump flag succeeded** OR **[BCP] set NVM manual RAM dump flag succeeded**

692	2024/06/19 21:32:01....	23.0060	172	ECU	SAFE	0	log	info	non...	3	[PMIC] Actual PMIC SOC PWRGOOD state = 0 , 0 = LOW, 1 = HIGH
693	2024/06/19 21:32:01....	23.0060	173	ECU	SAFE	0	log	info	non...	5	[SoC monitor] Actual XFLT INT state = 0 XFLT INT INV state = 1 , 0 = LOW, 1 = HIGH
694	2024/06/19 21:32:01....	23.1230	174	ECU	FS3I	0	log	info	non...	4	Channel 12 Available, handle 1
695	2024/06/19 21:32:01....	23.1240	175	ECU	FS3I	0	log	info	non...	4	Channel 12 Unavailable, handle 1
696	2024/06/19 21:32:01....	23.1260	176	ECU	BCP	0	log	info	non...	1	[BCP] set RTN RAM manual RAM dump flag succeeded
697	2024/06/19 21:32:01....	23.3690	177	ECU	SYST	0	log	info	non...	5	Heartbeat... 23369 : 153 (ms:us)
698	2024/06/19 21:32:01....	23.5060	178	ECU	SAFE	0	log	info	non...	5	Maximum duration between 2 SFI heartbeats is 50 ms 46 us
699	2024/06/19 21:32:01....	23.5060	179	ECU	SAFE	0	log	info	non...	3	[PMIC] Actual PMIC SOC PWRGOOD state = 0 , 0 = LOW, 1 = HIGH
700	2024/06/19 21:32:01....	23.5060	180	ECU	SAFE	0	log	info	non...	5	[SoC monitor] Actual XFLT INT state = 0 XFLT INT INV state = 1 , 0 = LOW, 1 = HIGH
701	2024/06/19 21:32:01....	23.7820	181	ECU	IOWD	0	log	info	non...	2	Command: 25

2. Initiate a Kernel panic - echo c > /proc/sysrq-trigger
3. Wait for MCU to detect heartbeat timeout from Node0 - This takes upto 25seconds.
   - Look for MCU DLT Trace - "IO WDG timeout occurred"

2163	2024/06/19 21:32:31....	53.6960	107	ECU	FS3I	0	log	warn	non...	4	[EVENT_TX_TIMEOUT] ESeq: 4 TSeq: 3
2164	2024/06/19 21:32:31....	53.7460	108	ECU	FS3I	0	log	warn	non...	2	I frame time out, handle 1
2165	2024/06/19 21:32:31....	53.7460	109	ECU	FS3I	0	log	warn	non...	4	[EVENT_TX_TIMEOUT] ESeq: 4 TSeq: 3
2166	2024/06/19 21:32:31....	53.7960	110	ECU	FS3I	0	log	warn	non...	2	I frame time out, handle 1
2167	2024/06/19 21:32:31....	53.7960	111	ECU	FS3I	0	log	warn	non...	4	[EVENT_TX_TIMEOUT] ESeq: 4 TSeq: 3
2168	2024/06/19 21:32:31....	53.8260	112	ECU	IOWD	0	log	warn	non...	1	IO WDG timeout occurred
2169	2024/06/19 21:32:31....	53.8260	113	ECU	IOWD	0	log	error	non...	2	Reset reason: 0
2170	2024/06/19 21:32:31....	53.8260	114	ECU	IOWD	0	log	info	non...	1	Starting warm reset procedure
2171	2024/06/19 21:32:31....	53.8260	115	ECU	SYST	0	log	info	non...	3	[UART] Set baudrate to 1000000 for NODE0 port
2172	2024/06/19 21:32:31....	53.8260	116	ECU	BCP	0	log	info	non...	3	[BCP] waiting for frame tag... (warm reset: 1)
2173	2024/06/19 21:32:31....	53.8270	117	ECU	FS3I	0	log	info	non...	3	Suspending FS3IPC instance 1 [0 - SFI, 1 - NODE0]
2174	2024/06/19 21:32:31....	53.8270	118	ECU	FS3I	0	log	info	non...	3	Suspending FS3IPC instance 0 [0 - SFI, 1 - NODE0]

4. MCU triggers a warm reset of SOC
   - Look for MCU DLT Trace - "Starting warm reset procedure"

2169	2024/06/19 21:32:31....	53.8260	113	ECU	IOWD	0	log	error	non...	2	Reset reason: 0
2170	2024/06/19 21:32:31....	53.8260	114	ECU	IOWD	0	log	info	non...	1	Starting warm reset procedure
2171	2024/06/19 21:32:31....	53.8260	115	ECU	SYST	0	log	info	non...	3	[UART] Set baudrate to 1000000 for NODE0 port

5. SOC requests MCU to send BCP frame

2280	2024/06/19 21:32:43....	65.5740	224	ECU	BCP	0	log	info	non...	1	[BCP] received fail frame (timeout)
2281	2024/06/19 21:32:43....	65.5760	225	ECU	BCP	0	log	info	non...	1	[BCP] received req frame
2282	2024/06/19 21:32:43....	65.5760	226	ECU	BCP	0	log	error	non...	1	Reading ethernet type failed or AD is the default one
2283	2024/06/19 21:32:43....	65.5760	227	ECU	BCP	0	log	info	non...	4	[BCP] manual RAM dump flags, retention RAM = 1 , NVM = 0

6. MCU sends BCP frame with request for small ram dump and starts a timeout of 15mins for completion of ram dump
   Look for MCU DLT Trace - "[BCP] sent response frame"

2287	2024/06/19 21:32:43....	65.5760	231	ECU	BCP	0	log	info	non...	1	[BCP] sent response frame
2288	2024/06/19 21:32:43....	65.5810	232	ECU	BCP	0	log	info	non...	1	[BCP] received ACK frame

7. LK enters fastboot mode
   - Check "Enumeration Success" on LK shell
8. Run scripts to trigger collection of ram dump

```
C:\Users\abudni\Desktop\PowerManagement\RamDumpTool\dumptool>python eautodump.py
================================================================
Mode: all
Domain: all
Section:  all
Output path: ./20240619-210332_virt_from_dram
================================================================
DRAM dump Mode
DSS Version : 0x1100000000011211
./20240619-210332_virt_from_dram/VM2_header_0xe0000000--0xe000ffff.lst...

ramdump start address is [0xe0000000]
ramdump size is [0x10000]
starting dump
================================================================
 RECEIVED:  100 %, read bytes: 0x00010000 |===================>|
================================================================

dump success

finished. total time: 0.047s
./20240619-210332_virt_from_dram/VM2_kernel_0xe0010000--0xe020ffff.lst...

ramdump start address is [0xe0010000]
ramdump size is [0x200000]
starting dump
================================================================
```

   commands: are same to run the script.
   for smalldump: python eautodump.py -m dss
   only kernel: python eautodump.py -s kernel
   full dump: python eautodump.py

9. Ramdump copied to host PC. (will be around 16 GB)

Scan2dram content validation

- When you pull the small dump / full ramdump from target you will have a file named: **SOC_scan2dram_0xebf00000–0xefafffff.lst**

Name	Date modified	Type	Size
SFI_log1_0xf6b00000--0xf6cfffff.lst	14-10-2024 05:26 PM	LST File	2,048 KB
SFI_log2_0xf6d00000--0xf6effffff.lst	14-10-2024 05:26 PM	LST File	2,048 KB
SOC_arraydump-panic_0xeac00000--0xebafffff.lst	14-10-2024 05:26 PM	LST File	15,360 KB
SOC_arraydump-reset_0xe9d00000--0xeabfffff.lst	14-10-2024 05:26 PM	LST File	15,360 KB
SOC_bcmdbg_0xebb00000--0xebeffffff.lst	14-10-2024 05:26 PM	LST File	4,096 KB
SOC_scan2dram_0xebf00000--0xefafffff.lst	14-10-2024 05:26 PM	LST File	61,440 KB
VM2_first_0xe0610000--0xe080ffff.lst	14-10-2024 05:26 PM	LST File	2,048 KB
VM2_header_0xe0000000--0xe000ffff.lst	14-10-2024 05:26 PM	LST File	64 KB
VM2_kernel_0xe0010000--0xe020ffff.lst	14-10-2024 05:26 PM	LST File	2,048 KB
VM2_kevent_0xe0810000--0xe0e0ffff.lst	14-10-2024 05:26 PM	LST File	6,144 KB
VM2_kmodule_0xe0e10000--0xe0e4ffff.lst	14-10-2024 05:26 PM	LST File	256 KB

- Now you can validate the contents of this file by following method.
  1. Check the lk log, if the “S2D Magic Detected - s2d sanity pass.” Is there means, you will get valid S2D dumps.

```
[2024-06-11 18:08:50.985] Core1: Hotplug
[2024-06-11 18:08:50.985] Core2: Hotplug
[2024-06-11 18:08:50.985] Core3: Hotplug
[2024-06-11 18:08:50.985] Core4: Hotplug
[2024-06-11 18:08:50.985] Core5: Hotplug
[2024-06-11 18:08:50.985] Core6: Hotplug
[2024-06-11 18:08:50.985] Core7: Hotplug
[2024-06-11 18:08:50.985] Core stat at previous(KERNEL)
[2024-06-11 18:08:51.002] ------------------------------------------------------------
[2024-06-11 18:08:51.002] Warm Reset Detected.
[2024-06-11 18:08:51.497] S2D Magic Detected - s2d sanity pass.
[2024-06-11 18:08:51.545] Host0 Lun1 has no gpt
[2024-06-11 18:08:51.545] Host0 Lun2 has no gpt
[2024-06-11 18:08:51.593] Host0 Lun1 has no gpt
[2024-06-11 18:08:51.593] Host0 Lun2 has no gpt
```

  2. From the hex S2D file, if the file has the marker “fd 0d 81 e9” twice in it, then the extracted S2D dump is valid too. Like below in this file case:

     $ hd SOC_scan2dram_0xebf00000--0xefafffff.lst | grep "fd 0d 81 e9"

     027aafe0 fd 0d 81 e9 fd 0d 81 e9 ca d5 00 a6 1d 1d 55 b0 |.....U.|