```
From a8ce4d0eb6410754716657d6045cea4cc59acb20 Mon Sep 17 00:00:00 2001
From: Gabriel <gshahrouzi@gmail.com>
Date: Sun, 23 Feb 2025 21:49:31 -0500
Subject: [PATCH] Decode stacktrace

Complete decode stacktrace task. Find bug on syzkaller.appspot.com and
decode the call trace.

Signed-off-by: Gabriel <gshahrouzi@gmail.com>
---
 decode-stacktrace/decode_stacktrace.txt | 19 ++++++++++++++++++
 decode-stacktrace/report.txt            | 15 +++++++++++++++
 decode-stacktrace/stacktrace.txt        | 19 ++++++++++++++++++
 3 files changed, 53 insertions(+)
 create mode 100644 decode-stacktrace/decode_stacktrace.txt
 create mode 100644 decode-stacktrace/report.txt
 create mode 100644 decode-stacktrace/stacktrace.txt

diff --git a/decode-stacktrace/decode_stacktrace.txt b/decode-stacktrace/decode_stacktrace.
txt
new file mode 100644
index 0000000..d262ca4
--- /dev/null
+++ b/decode-stacktrace/decode_stacktrace.txt
@@ -0,0 +1,19 @@
+Call trace:
+efivarfs_pm_notify+0xcc/0x350 480 (P)
+notifier_call_chain+0x1c4/0x550 85
+notifier_call_chain_robust kernel/notifier.c:120 [inline]
+blocking_notifier_call_chain_robust+0xdc/0x1bc 345
+pm_notifier_call_chain_robust+0x34/0x64 102
+snapshot_open+0x11c/0x270 87
+misc_open+0x2b8/0x328 179
+chrdev_open+0x3b0/0x4bc 414
+do_dentry_open+0xb7c/0x1538 956
+vfs_open+0x48/0x2d8 1086
+do_open fs/namei.c:3830 [inline]
+path_openat+0x2308/0x2b1c 3989
+do_filp_open+0x1e8/0x404 4016
+do_sys_openat2+0x124/0x1b8 1428
+do_sys_open fs/open.c:1443 [inline]
+__do_sys_openat fs/open.c:1459 [inline]
+__se_sys_openat fs/open.c:1454 [inline]
+__arm64_sys_openat+0x1f0/0x240 1454
diff --git a/decode-stacktrace/report.txt b/decode-stacktrace/report.txt
new file mode 100644
index 0000000..8620982
--- /dev/null
+++ b/decode-stacktrace/report.txt
@@ -0,0 +1,15 @@
+Used gabriel-shahrouzi@gabriel-shahrouzi-Virtual-Machine:/opt/linux_work/kernel_modules/de
code-stac
+ktrace$                            ../../linux_mainline/scripts/decode_sta
+cktrace.sh ../../linux_mainline/vmlinux auto < /opt/linux_work/kernel_modules/decode-stack
trace/stacktrace.txt
+to decode stacktrace from https://syzkaller.appspot.com/bug?extid=00d13e505ef530a45100.
+However, there was no need to decode as it seems it was already decoded in the bug report.
 I went to
+another bug report and they had the decoded output for the stack trace as well. This is ni
ce because
+from the sample crash report for a bug, I can visit different files that were evoked as we
ll as the
+specific line numbers for them. Clicking on it takes me to the git.kernel.org page and lao
ds the page
+to the line number that was referenced. Not sure what to do with this information as there
 are a lot of
+files that were called and the stack trace is decently long.
+
```

```
+Quite confusing when first looking at the page because there is a lot of information prese
nt
+on the page. I will have to look at what the bottom part is as it seems to be doing backup
s of kernels
+with specified time below. It doesn’t look like it has anything to do with the actual bug
and seems to
+be separate but complemtary to what’s on the top part of the page for the bug report.
\ No newline at end of file
diff --git a/decode-stacktrace/stacktrace.txt b/decode-stacktrace/stacktrace.txt
new file mode 100644
index 0000000..41ba52d
--- /dev/null
+++ b/decode-stacktrace/stacktrace.txt
@@ -0,0 +1,19 @@
+Call trace:
+ efivarfs_pm_notify+0xcc/0x350 fs/efivarfs/super.c:480 (P)
+ notifier_call_chain+0x1c4/0x550 kernel/notifier.c:85
+ notifier_call_chain_robust kernel/notifier.c:120 [inline]
+ blocking_notifier_call_chain_robust+0xdc/0x1bc kernel/notifier.c:345
+ pm_notifier_call_chain_robust+0x34/0x64 kernel/power/main.c:102
+ snapshot_open+0x11c/0x270 kernel/power/user.c:87
+ misc_open+0x2b8/0x328 drivers/char/misc.c:179
+ chrdev_open+0x3b0/0x4bc fs/char_dev.c:414
+ do_dentry_open+0xb7c/0x1538 fs/open.c:956
+ vfs_open+0x48/0x2d8 fs/open.c:1086
+ do_open fs/namei.c:3830 [inline]
+ path_openat+0x2308/0x2b1c fs/namei.c:3989
+ do_filp_open+0x1e8/0x404 fs/namei.c:4016
+ do_sys_openat2+0x124/0x1b8 fs/open.c:1428
+ do_sys_open fs/open.c:1443 [inline]
+ __do_sys_openat fs/open.c:1459 [inline]
+ __se_sys_openat fs/open.c:1454 [inline]
+ __arm64_sys_openat+0x1f0/0x240 fs/open.c:1454
--
2.45.2
```