



author Henry Martin <bsdhenrymartin@gmail.com> 2025-04-09 20:48:13 +0800  
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2025-05-02 08:01:35 +0200  
commit [01e86ea22610d98ae6141e428019a6916e79f725](#) (patch)  
tree [be7751b31f0c1bdb8f21dd2c4603fe5ca7aec0e2](#)  
parent [02ac36a77d260ab4a1aad4feb9d16defc908fc0b](#) (diff)  
download [linux-01e86ea22610d98ae6141e428019a6916e79f725.tar.gz](#)

## diff options

context:   
space:   
mode:

## cpufreq: apple-soc: Fix null-ptr-deref in apple\_soc\_cpufreq\_get\_rate()

[ Upstream commit 9992649f6786921873a9b89dafa5e04d8c5fef2b ]

cpufreq\_cpu\_get\_raw() can return NULL when the target CPU is not present in the policy->cpus mask. apple\_soc\_cpufreq\_get\_rate() does not check for this case, which results in a NULL pointer dereference.

Fixes: 6286bbb40576 ("cpufreq: apple-soc: Add new driver to control Apple SoC CPU P-states")  
Signed-off-by: Henry Martin <bsdhenrymartin@gmail.com>  
Signed-off-by: Viresh Kumar <viresh.kumar@linaro.org>  
Signed-off-by: Sasha Levin <sashal@kernel.org>

## Diffstat

|            |                                                     |    |
|------------|-----------------------------------------------------|----|
| -rw-r--r-- | <a href="#">drivers/cpufreq/apple-soc-cpufreq.c</a> | 10 |
|------------|-----------------------------------------------------|----|

1 files changed, 8 insertions, 2 deletions

diff --git a/drivers/cpufreq/apple-soc-cpufreq.c b/drivers/cpufreq/apple-soc-cpufreq.c

index 269b18c62d0402..82007f6a24d2a8 100644

--- a/drivers/cpufreq/apple-soc-cpufreq.c

+++ b/drivers/cpufreq/apple-soc-cpufreq.c

@@ -134,11 +134,17 @@ static const struct of\_device\_id apple\_soc\_cpufreq\_of\_match[] \_\_maybe\_unused = {

```
static unsigned int apple_soc_cpufreq_get_rate(unsigned int cpu)
{
-     struct cpufreq_policy *policy = cpufreq_cpu_get_raw(cpu);
-     struct apple_cpu_priv *priv = policy->driver_data;
+     struct cpufreq_policy *policy;
+     struct apple_cpu_priv *priv;
+     struct cpufreq_frequency_table *p;
+     unsigned int pstate;

+     policy = cpufreq_cpu_get_raw(cpu);
+     if (unlikely(!policy))
+         return 0;
+     priv = policy->driver_data;

    if (priv->info->cur_pstate_mask) {
        u32 reg = readl_relaxed(priv->reg_base + APPLE_DVFS_STATUS);
```