author	Henry Martin <bsdhenrymartin@gmail.com>	2025-04-09 20:48:13 +0800
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2025-05-02 07:50:42 +0200
commit	1053dcf8a504d4933bb3f73df22bc363298d194b (patch)	
tree	0f98bd5248f699ef200768cfa93f2c946c8a613e	
parent	92d55d7051833116af0fc8664599f458e3dfa858 (diff)	
download	linux-1053dcf8a504d4933bb3f73df22bc363298d194b.tar.gz	

diff options

context: 3

space: include

mode: unified

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--	drivers/cpufreq/apple-soc-cpufreq.c	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 021f423705e1b1..9ba6b09775f617 100644
--- a/drivers/cpufreq/apple-soc-cpufreq.c
+++ b/drivers/cpufreq/apple-soc-cpufreq.c
@@ -103,11 +103,17 @@ static const struct of_device_id apple_soc_cpufreq_of_match[] = {

 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) {
                u64 reg = readq_relaxed(priv->reg_base + APPLE_DVFS_STATUS);
```