



authorHenry Martin <bsdhenrymartin@gmail.com>2025-04-08 23:03:54 +0800

committerGreg Kroah-Hartman <gregkh@linuxfoundation.org>2025-05-02 07:44:29 +0200

commit8fbaa76690f67a7cbad315f89d607b46e3e06ede(patch)

treea7d07ef95aaab12a1b9455dcb5654ab84c068ac7

parent4e3d1c1925d8e752992cd893d03d974e6807ac16(diff)

downloadlinux-8fbaa76690f67a7cbad315f89d607b46e3e06ede.tar.gz

diff options

context:

3

space:

include

mode:

unified

cpufreq: scpi: Fix null-ptr-deref in scpi_cpufreq_get_rate()

[Upstream commit 73b24dc731731edf762f9454552cb3a5b7224949]

cpufreq_cpu_get_raw() can return NULL when the target CPU is not present in the policy->cpus mask. scpi_cpufreq_get_rate() does not check for this case, which results in a NULL pointer dereference.

Fixes: 343a8d17fa8d ("cpufreq: scpi: remove arm_big_little dependency")
Signed-off-by: Henry Martin <bsdhenrymartin@gmail.com>
Acked-by: Sudeep Holla <sudeep.holla@arm.com>
Signed-off-by: Viresh Kumar <viresh.kumar@linaro.org>
Signed-off-by: Sasha Levin <sashal@kernel.org>

Diffstat

-rw-r--r--	drivers/cpufreq/scpi-cpufreq.c	13
------------	--------------------------------	----

1 files changed, 10 insertions, 3 deletions

```
diff --git a/drivers/cpufreq/scpi-cpufreq.c b/drivers/cpufreq/scpi-cpufreq.c
index 35b20c74dbfc7e..f111f1f3bf38db 100644
--- a/drivers/cpufreq/scpi-cpufreq.c
+++ b/drivers/cpufreq/scpi-cpufreq.c
@@ -37,9 +37,16 @@ static struct scpi_ops *scpi_ops;

static unsigned int scpi_cpufreq_get_rate(unsigned int cpu)
{
-     struct cpufreq_policy *policy = cpufreq_cpu_get_raw(cpu);
-     struct scpi_data *priv = policy->driver_data;
-     unsigned long rate = clk_get_rate(priv->clk);
+     struct cpufreq_policy *policy;
+     struct scpi_data *priv;
+     unsigned long rate;
+
+     policy = cpufreq_cpu_get_raw(cpu);
+     if (unlikely(!policy))
+         return 0;
+
+     priv = policy->driver_data;
+     rate = clk_get_rate(priv->clk);

    return rate / 1000;
}
```