



author Henry Martin <bsdhenrymartin@gmail.com> 2025-04-08 23:03:53 +0800
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2025-05-02 08:01:35 +0200
commit cfaca93b8fe317b7faa9af732e0ba8c9081fa018 (patch)
tree 8160a19584564070d8d3ddb258113c0e38ec72dd
parent 01e86ea22610d98ae6141e428019a6916e79f725 (diff)
download linux-cfaca93b8fe317b7faa9af732e0ba8c9081fa018.tar.gz

diff options

context: 3 ▼
space: include ▼
mode: unified ▼

cpufreq: scmi: Fix null-ptr-deref in scmi_cpufreq_get_rate()

[Upstream commit 484d3f15cc6cbaa52541d6259778e715b2c83c54]

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

Add NULL check after cpufreq_cpu_get_raw() to prevent this issue.

Fixes: 99d6bdf33877 ("cpufreq: add support for CPU DVFS based on SCMI message protocol")

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/scmi-cpufreq.c	10
------------	--------------------------------	----

1 files changed, 8 insertions, 2 deletions

diff --git a/drivers/cpufreq/scmi-cpufreq.c b/drivers/cpufreq/scmi-cpufreq.c

index 914bf2c940a037..9c6eb1238f1be3 100644

--- a/drivers/cpufreq/scmi-cpufreq.c

+++ b/drivers/cpufreq/scmi-cpufreq.c

@@ -37,11 +37,17 @@ static struct cpufreq_driver scmi_cpufreq_driver;

```
static unsigned int scmi_cpufreq_get_rate(unsigned int cpu)
{
-     struct cpufreq_policy *policy = cpufreq_cpu_get_raw(cpu);
-     struct scmi_data *priv = policy->driver_data;
+     struct cpufreq_policy *policy;
+     struct scmi_data *priv;
+     unsigned long rate;
+     int ret;

+     policy = cpufreq_cpu_get_raw(cpu);
+     if (unlikely(!policy))
+         return 0;

+     priv = policy->driver_data;

+     ret = perf_ops->freq_get(ph, priv->domain_id, &rate, false);
```

```
if (ret)
    return 0;
```