author	Cong Wang <xiyou.wangcong@gmail.com>	2025-04-17 11:47:31 -0700
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2025-05-02 07:59:02 +0200
commit	c6f035044104c6ff656f4565cd22938dc892528c (patch)	
tree	3cd0812d3956b91abbf77af3cb6416b9399bb5fa	
parent	86cd4641c713455a4f1c8e54c370c598c2b1cee0 (diff)	
download	linux-c6f035044104c6ff656f4565cd22938dc892528c.tar.gz	

net_sched: hfsc: Fix a potential UAF in hfsc_dequeue() too

```
[ Upstream commit 6ccbda44e2cc3d26fd22af54c650d6d5d801addf ]

Similarly to the previous patch, we need to safe guard hfsc_dequeue()
too. But for this one, we don't have a reliable reproducer.

Fixes: 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 ("Linux-2.6.12-rc2")
Reported-by: Gerrard Tai <gerrard.tai@starlabs.sg>
Signed-off-by: Cong Wang <xiyou.wangcong@gmail.com>
Reviewed-by: Jamal Hadi Salim <jhs@mojatatu.com>
Link: https://patch.msgid.link/20250417184732.943057-3-xiyou.wangcong@gmail.com
Signed-off-by: Jakub Kicinski <kuba@kernel.org>
Signed-off-by: Sasha Levin <sashal@kernel.org>
```

Diffstat

-rw-r--r-- net/sched/sch_hfsc.c 14

1 files changed, 10 insertions, 4 deletions

```
diff --git a/net/sched/sch_hfsc.c b/net/sched/sch_hfsc.c
index e730d3f791c24d..5bb4ab9941d6e9 100644
--- a/net/sched/sch_hfsc.c
+++ b/net/sched/sch_hfsc.c
@@ -1637,10 +1637,16 @@ hfsc_dequeue(struct Qdisc *sch)
                if (cl->qdisc->q.qlen != 0) {
                        /* update ed */
                        next_len = qdisc_peek_len(cl->qdisc);
-                       if (realtime)
-                               update_ed(cl, next_len);
-                       else
-                               update_d(cl, next_len);
+                       /* Check queue length again since some qdisc implementations
+                        * (e.g., netem/codel) might empty the queue during the peek
+                        * operation.
+                        */
+                       if (cl->qdisc->q.qlen != 0) {
+                               if (realtime)
+                                       update_ed(cl, next_len);
+                               else
+                                       update_d(cl, next_len);
+                       }
                } else {
                        /* the class becomes passive */
```

```
eltree_remove(cl);
```