**Description**

**CID 1465663: Null pointer dereferences (FORWARD_NULL)**

```c
/* since fb lock is still held this flow won't be found until we are done */
FLOWLOCK_UNLOCK(old_f);

/* Get a new flow. It will be either a locked flow or NULL */
>>> CID 1465663: Null pointer dereferences (FORWARD_NULL)
>>> Passing "fls" to "FlowGetNew", which dereferences null "fls->dtv".
Flow *f = FlowGetNew(tv, fls, p);
if (f == NULL) {
    return NULL;
}
/* flow is locked */
```

**CID 1465660: Program hangs (LOCK)**

```c
static uint32_t FlowTimeoutHashInChunks(FlowManagerTimeoutThread *td,
    struct timeval *ts,
    const uint32_t hash_min, const uint32_t hash_max,
)
```

**CID 1465659: Null pointer dereferences (FORWARD_NULL)**

```c
static uint32_t FlowTimeoutHashInChunks(FlowManagerTimeoutThread *td,
    struct timeval *ts,
    const uint32_t hash_min, const uint32_t hash_max,
```
/src/flow-hash.c: 1098 in FlowGetUsedFlow()
1092 (void)OutputFlowLog(tv, dtv->output_flow_thread_data, f);
1093
1094 FlowClearMemory(f, f->protomap);
1095
1096 /* leave locked */
1097
>>> CID 1465659: Null pointer dereferences (FORWARD_NULL)
>>> Dereferencing null pointer "dtv".
1098 STATSADDUI64(counter_flow_get_used_eval, tried);
1099 return f;
1100 }
1101
1102 STATSADDUI64(counter_flow_get_used_failed, 1);
1103 return NULL;

** CID 1465658: Control flow issues (DEADCODE)
/src/flow-hash.c: 517 in FlowSpareSync()

```c
#define UNITTESTS

if (spare_sync) {
    StatsAddUI64(tv, fls->dtv->counter_flow_spare_sync_avg, fls->spare_queue.len+1);
} else if (f != NULL) {
    StatsAddUI64(tv, fls->dtv->counter_flow_spare_sync_empty);
>>> CID 1465658: Control flow issues (DEADCODE)
>>> Execution cannot reach the expression "fls->spare_queue.len < 99U" inside this statement: "if (f != NULL && fls->spare..."
} else if (f != NULL && fls->spare_queue.len < 99) {
    StatsIncr(tv, fls->dtv->counter_flow_spare_sync_incomplete);
} else {
    StatsIncr(tv, fls->dtv->counter_flow_spare_sync);
}
#endif
```

---

History
#1 - 08/26/2020 05:45 AM - Victor Julien

https://github.com/OISF/suricata/pull/5325 fixes all but the unlock one. That is a FP, so I need to suppress it. Leaving the ticket open for now.