README.md

Open5gs - Malformated UE initial message crashes AMF causing DoS

Recently, we discovered a vulnerability that may cause Open5gs AMF to crash during a code audit of Open5gs Ver2.4.11. The specific causes of the vulnerability are as follows:

Vulnerability description

When processing UE attachment, a memory leak in AMF `ngap-handler.c` from open5gs causing a DoS vulnerability.

ngap-handler

UE initial message is handled by function `ngap_handle_initial_ue_message` from `src/amf/ngap-handler.c` .

> src/amf/ngap-handler.c

```
void ngap_handle_initial_ue_message(amf_gnb_t *gnb, ogs_ngap_message_t *message)
{
```

```
...
```

`RAN_UE_NGAP_ID` and `UserLocationInformation` is extracted from `InitialUEMessage`.

```
for (i = 0; i < InitialUEMessage->protocolIEs.list.count; i++) {
    ie = InitialUEMessage->protocolIEs.list.array[i];
    switch (ie->id) {
    case NGAP_ProtocolIE_ID_id_RAN_UE_NGAP_ID:
        RAN_UE_NGAP_ID = &ie->value.choice.RAN_UE_NGAP_ID;
        break;
    case NGAP_ProtocolIE_ID_id_NAS_PDU:
        NAS_PDU = &ie->value.choice.NAS_PDU;
        break;
    case NGAP_ProtocolIE_ID_id_UserLocationInformation:
        UserLocationInformation =
            &ie->value.choice.UserLocationInformation;
        break;
    ...
```

`ran_ue` structure will be allocated and assigned after validating `RAN_UE_NGAP_ID` by calling `ran_ue_add`.

```
if (!RAN_UE_NGAP_ID) {
    ogs_error("No RAN_UE_NGAP_ID");
    ogs_assert(OGS_OK ==
        ngap_send_error_indication(gnb, NULL, NULL,
            NGAP_Cause_PR_protocol, NGAP_CauseProtocol_semantic_error));
    return;
}

ran_ue = ran_ue_find_by_ran_ue_ngap_id(gnb, *RAN_UE_NGAP_ID);
if (!ran_ue) {
    ran_ue = ran_ue_add(gnb, *RAN_UE_NGAP_ID);
    ogs_assert(ran_ue);
    ...
```

If `UserLocationInformation` is not present, the function will return and `ran_ue_remove` will never be called, here is the memory leak bug.

```
if (!UserLocationInformation) {
    ogs_error("No UserLocationInformation");
    ogs_assert(OGS_OK ==
        ngap_send_error_indication(gnb, &ran_ue->ran_ue_ngap_id, NULL,
```

```
                NGAP_Cause_PR_protocol, NGAP_CauseProtocol_semantic_error));
        return;
    }
    ...
}
```

UE_ADD UE_POOL

Pool `ran_ue_pool` is initialed by `amf_context_init` from `src/amf/context.c` on line 61.

> src/amf/context.c

```
    ogs_pool_init(&ran_ue_pool, ogs_app()->max.ue);
```

When calling `ran_ue_add`, `ran_ue` will be allocated.

```
ran_ue_t *ran_ue_add(amf_gnb_t *gnb, uint32_t ran_ue_ngap_id)
{
    ran_ue_t *ran_ue = NULL;

    ogs_assert(gnb);

    ogs_pool_alloc(&ran_ue_pool, &ran_ue);
    ogs_assert(ran_ue);
    memset(ran_ue, 0, sizeof *ran_ue);
    ...


    ogs_list_add(&gnb->ran_ue_list, ran_ue);

    stats_add_ran_ue();

    return ran_ue;
}
```

One must call `ran_ue_remove` after ue_add to free the `ran_ue`.

```
void ran_ue_remove(ran_ue_t *ran_ue)
{
    ogs_assert(ran_ue);
    ogs_assert(ran_ue->gnb);

    ogs_list_remove(&ran_ue->gnb->ran_ue_list, ran_ue);
```

```
    ogs_assert(ran_ue->t_ng_holding);
    ogs_timer_delete(ran_ue->t_ng_holding);

    ogs_pool_free(&ran_ue_pool, ran_ue);

    stats_remove_ran_ue();
}
```

`max.ue` is defined 1024 as default.

> lib/ogs-context.c

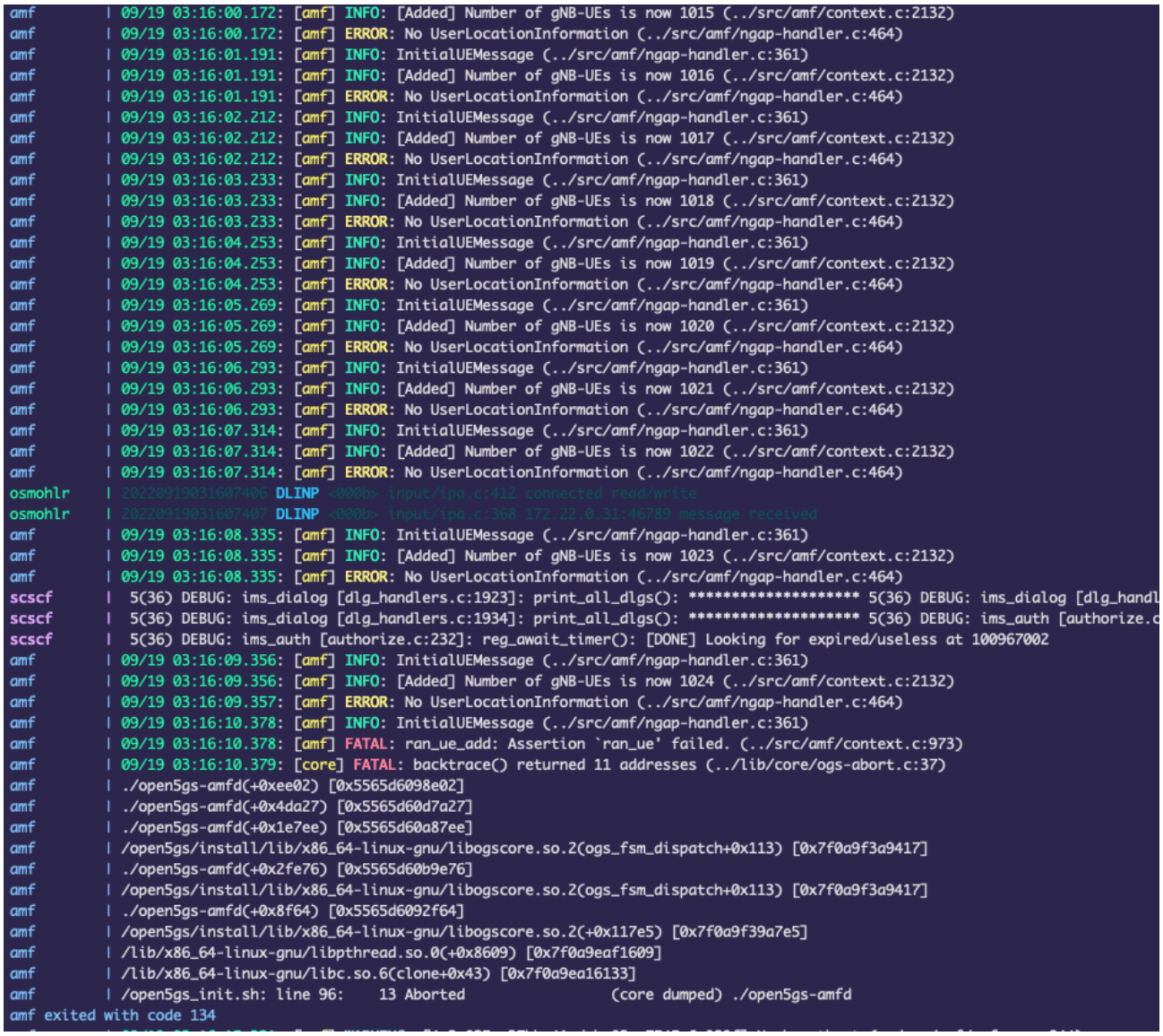
```
static void app_context_prepare(void)
{
    ...

#define MAX_NUM_OF_UE               1024    /* Num of UEs */
#define MAX_NUM_OF_PEER             64      /* Num of Peer */

    self.max.ue = MAX_NUM_OF_UE;
    ...
}
```

POC

To trigger this vulnerability, an `InitialUEMessage` without `UserLocationInformation` needs to be build.

```
[2022-09-19 03:16:03.232] [rrc] [info] RRC Setup for UE[1021]
[2022-09-19 03:16:03.232] [ngap] [debug] Initial NAS message received from UE[1021]
[2022-09-19 03:16:03.233] [ngap] [error] Error indication received. Cause: protocol/semantic-error
[2022-09-19 03:16:04.034] [rls] [debug] UE[1018] signal lost
[2022-09-19 03:16:04.250] [rrc] [debug] UE[1022] new signal detected
[2022-09-19 03:16:04.251] [rrc] [info] RRC Setup for UE[1022]
[2022-09-19 03:16:04.252] [ngap] [debug] Initial NAS message received from UE[1022]
[2022-09-19 03:16:04.253] [ngap] [error] Error indication received. Cause: protocol/semantic-error
[2022-09-19 03:16:05.053] [rls] [debug] UE[1019] signal lost
[2022-09-19 03:16:05.053] [rls] [debug] UE[1020] signal lost
[2022-09-19 03:16:05.267] [rrc] [debug] UE[1023] new signal detected
[2022-09-19 03:16:05.268] [rrc] [info] RRC Setup for UE[1023]
[2022-09-19 03:16:05.268] [ngap] [debug] Initial NAS message received from UE[1023]
[2022-09-19 03:16:05.269] [ngap] [error] Error indication received. Cause: protocol/semantic-error
[2022-09-19 03:16:06.290] [rrc] [debug] UE[1024] new signal detected
[2022-09-19 03:16:06.292] [rrc] [info] RRC Setup for UE[1024]
[2022-09-19 03:16:06.292] [ngap] [debug] Initial NAS message received from UE[1024]
[2022-09-19 03:16:06.293] [ngap] [error] Error indication received. Cause: protocol/semantic-error
[2022-09-19 03:16:07.094] [rls] [debug] UE[1021] signal lost
[2022-09-19 03:16:07.311] [rrc] [debug] UE[1025] new signal detected
[2022-09-19 03:16:07.313] [rrc] [info] RRC Setup for UE[1025]
[2022-09-19 03:16:07.313] [ngap] [debug] Initial NAS message received from UE[1025]
[2022-09-19 03:16:07.314] [ngap] [error] Error indication received. Cause: protocol/semantic-error
[2022-09-19 03:16:08.115] [rls] [debug] UE[1022] signal lost
[2022-09-19 03:16:08.333] [rrc] [debug] UE[1026] new signal detected
[2022-09-19 03:16:08.334] [rrc] [info] RRC Setup for UE[1026]
[2022-09-19 03:16:08.335] [ngap] [debug] Initial NAS message received from UE[1026]
[2022-09-19 03:16:08.336] [ngap] [error] Error indication received. Cause: protocol/semantic-error
[2022-09-19 03:16:09.136] [rls] [debug] UE[1023] signal lost
[2022-09-19 03:16:09.354] [rrc] [debug] UE[1027] new signal detected
[2022-09-19 03:16:09.355] [rrc] [info] RRC Setup for UE[1027]
[2022-09-19 03:16:09.356] [ngap] [debug] Initial NAS message received from UE[1027]
[2022-09-19 03:16:09.357] [ngap] [error] Error indication received. Cause: protocol/semantic-error
[2022-09-19 03:16:10.157] [rls] [debug] UE[1024] signal lost
[2022-09-19 03:16:10.375] [rrc] [debug] UE[1028] new signal detected
[2022-09-19 03:16:10.377] [rrc] [info] RRC Setup for UE[1028]
[2022-09-19 03:16:10.377] [ngap] [debug] Initial NAS message received from UE[1028]
[2022-09-19 03:16:10.601] [sctp] [debug] SCTP association shutdown (clientId: 2)
[2022-09-19 03:16:10.601] [sctp] [warning] Unhandled SCTP notification received
[2022-09-19 03:16:10.601] [ngap] [error] Association terminated for AMF[2]
[2022-09-19 03:16:10.601] [ngap] [debug] Removing AMF context[2]
[2022-09-19 03:16:11.179] [rls] [debug] UE[1025] signal lost
[2022-09-19 03:16:11.397] [rrc] [debug] UE[1029] new signal detected
[2022-09-19 03:16:11.399] [rrc] [info] RRC Setup for UE[1029]
[2022-09-19 03:16:11.399] [ngap] [debug] Initial NAS message received from UE[1029]
[2022-09-19 03:16:11.399] [ngap] [error] AMF selection for UE[1029] failed. Could not find a suitable AMF.
[2022-09-19 03:16:11.399] [ngap] [error] AMF context not found with id: 0
```

AMF will crash after 1024 malformated UE initial messages is reached.



Upadate

We have reported this vulnerability to the vendor through email at 19 Sep 2022, but this bug has not been fixed yet.

Acknowledgment

Credit to @ToughRunner,@HenryzhaoH,@leonW7 from Shanghai Jiao Tong University.

Releases

No releases published

Packages

No packages published