README.md

Open5gs AMF DOS Vulnerability

Recently, we discovered a logic vulnerability that may cause Open5gs AMF to crash during a code audit of Open5gs Ver2.4.9. The specific causes of the vulnerability are as follows:

Vulnerability description

When AMF is initialized, the default maximum number of GNB per AMF/MME is defined to 64.

> /lib/app/ogs-context.c

```
#define MAX_NUM_OF_UE               1024    /* Num of UE per AMF/MME */
#define MAX_NUM_OF_GNB              64      /* Num of gNB per AMF/MME */

    self.max.gnb = MAX_NUM_OF_GNB;
    self.max.ue = MAX_NUM_OF_UE;
```

Memory pool is initialized according to the maximum value defined before.

> /src/amf/context.c

```
    /* Allocate TWICE the pool to check if maximum number of gNBs is reached */
    ogs_pool_init(&amf_gnb_pool, ogs_app()->max.gnb*2);
```

The request should fail when the NR initiates an `NG_Setup_Request` request to the core network if the maximum value of `NG_Setup_Request` is exceeded

```
    if (maximum_number_of_gnbs_is_reached()) {
        ogs_warn("NG-Setup failure:");
        ogs_warn("    Maximum number of gNBs reached");
        group = NGAP_Cause_PR_misc;
        cause = NGAP_CauseMisc_control_processing_overload;

        ogs_assert(OGS_OK ==
            ngap_send_ng_setup_failure(gnb, group, cause));
        return;
    }
```

However, the moment SCTP connection successfully established, `amf_gnb_t` structure is allocated and added to the list before any check.

> /src/amf/ngap-sctp.c

```
static void lksctp_accept_handler(short when, ogs_socket_t fd, void *data)
{
    ogs_assert(data);
    ogs_assert(fd != INVALID_SOCKET);

    ngap_accept_handler(data);
}
void ngap_accept_handler(ogs_sock_t *sock)
{
    char buf[OGS_ADDRSTRLEN];
    ogs_sock_t *new = NULL;
    ogs_assert(sock);
    new = ogs_sock_accept(sock);
    if (new) {
        ...

        ngap_event_push(AMF_EVT_NGAP_LO_ACCEPT,
                new, addr, NULL, 0, 0);
        ...
    } else {
        ogs_log_message(OGS_LOG_ERROR, ogs_socket_errno, "accept() failed");
    }
}
```

> /src/amf/amf-context.c

```
    case AMF_EVT_NGAP_LO_ACCEPT:
        sock = e->ngap.sock;
        ogs_assert(sock);
        addr = e->ngap.addr;
        ogs_assert(addr);

        ogs_info("gNB-N2 accepted[%s] in master_sm module",
            OGS_ADDR(addr, buf));

        gnb = amf_gnb_find_by_addr(addr);
        if (!gnb) {
            gnb = amf_gnb_add(sock, addr);
            ogs_assert(gnb);
        } else {
            ogs_warn("gNB context duplicated with IP-address [%s]!!!",
                    OGS_ADDR(addr, buf));
            ogs_sock_destroy(sock);
            ogs_free(addr);
            ogs_warn("N2 Socket Closed");
        }

        break;
```

Function `amf_gnb_find_by_addr` performs a detection and does not allow the same IP to initiate multiple gNB Contexts, the detection function searches through the hash value of the ogs_sockaddr_t structure, so SCTP connections initiated by different ports of the same IP will also bypass this detection restriction.

Function `amf_gnb_find_by_addr` performs a detection using the hash value of `ogs_sockaddr_t` structure, which includes port number, so new SCTP connections initialed by different ports from the same IP address will be treated as a new one. Therefore, the cost of this attack is very low.

```
amf_gnb_t *amf_gnb_find_by_addr(ogs_sockaddr_t *addr)
{
    ogs_assert(addr);
    return (amf_gnb_t *)ogs_hash_get(self.gnb_addr_hash,
            addr, sizeof(ogs_sockaddr_t));

    return NULL;
}
```

In result, when an attacker initiates multiple NG setup requests, AMF will crash.

POC

```
amf         | 08/03 02:29:51.983: [amf] INFO: gNB-N2 accepted[172.22.0.23]:38374 in ng-path module (../src/
amf/ngap-sctp.c:113)
amf         | 08/03 02:29:51.983: [amf] INFO: gNB-N2 accepted[172.22.0.23] in master_sm module (../src/amf/
amf-sm.c:621)
amf         | 08/03 02:29:51.983: [amf] INFO: [Added] Number of gNBs is now 126 (../src/amf/context.c:877)
amf         | 08/03 02:29:51.984: [amf] INFO: gNB-N2[172.22.0.23] max_num_of_ostreams : 10 (../src/amf/amf-
sm.c:660)
amf         | 08/03 02:29:51.984: [amf] WARNING: NG-Setup failure: (../src/amf/ngap-handler.c:283)
amf         | 08/03 02:29:51.984: [amf] WARNING:     Maximum number of gNBs reached (../src/amf/ngap-handle
r.c:284)
amf         | 08/03 02:29:53.217: [amf] INFO: gNB-N2 accepted[172.22.0.23]:52474 in ng-path module (../src/
amf/ngap-sctp.c:113)
amf         | 08/03 02:29:53.217: [amf] INFO: gNB-N2 accepted[172.22.0.23] in master_sm module (../src/amf/
amf-sm.c:621)
amf         | 08/03 02:29:53.217: [amf] INFO: [Added] Number of gNBs is now 127 (../src/amf/context.c:877)
amf         | 08/03 02:29:53.217: [amf] INFO: gNB-N2[172.22.0.23] max_num_of_ostreams : 10 (../src/amf/amf-
sm.c:660)
amf         | 08/03 02:29:53.218: [amf] WARNING: NG-Setup failure: (../src/amf/ngap-handler.c:283)
amf         | 08/03 02:29:53.218: [amf] WARNING:     Maximum number of gNBs reached (../src/amf/ngap-handle
r.c:284)
amf         | 08/03 02:29:54.066: [amf] INFO: gNB-N2 accepted[172.22.0.23]:57764 in ng-path module (../src/
amf/ngap-sctp.c:113)
amf         | 08/03 02:29:54.066: [amf] INFO: gNB-N2 accepted[172.22.0.23] in master_sm module (../src/amf/
amf-sm.c:621)
amf         | 08/03 02:29:54.066: [amf] INFO: [Added] Number of gNBs is now 128 (../src/amf/context.c:877)
amf         | 08/03 02:29:54.066: [amf] INFO: gNB-N2[172.22.0.23] max_num_of_ostreams : 10 (../src/amf/amf-
sm.c:660)
amf         | 08/03 02:29:54.068: [amf] WARNING: NG-Setup failure: (../src/amf/ngap-handler.c:283)
amf         | 08/03 02:29:54.068: [amf] WARNING:     Maximum number of gNBs reached (../src/amf/ngap-handle
r.c:284)
amf         | 08/03 02:29:55.182: [amf] INFO: gNB-N2 accepted[172.22.0.23]:53436 in ng-path module (../src/
amf/ngap-sctp.c:113)
amf         | 08/03 02:29:55.182: [amf] INFO: gNB-N2 accepted[172.22.0.23] in master_sm module (../src/amf/
amf-sm.c:621)
amf         | 08/03 02:29:55.182: [amf] FATAL: amf_gnb_add: Assertion `gnb' failed. (../src/amf/context.c:8
45)
amf         | 08/03 02:29:55.183: [core] FATAL: backtrace() returned 8 addresses (../lib/core/ogs-abort.c:3
7)
amf         | ./open5gs-amfd(+0xd24e) [0x55cb6de3f24e]
amf         | ./open5gs-amfd(+0x307e5) [0x55cb6de627e5]
amf         | /open5gs/install/lib/x86_64-linux-gnu/libogscore.so.2(ogs_fsm_dispatch+0xab) [0x7f520e5e4cc7]
amf         | ./open5gs-amfd(+0x7e69) [0x55cb6de39e69]
amf         | /open5gs/install/lib/x86_64-linux-gnu/libogscore.so.2(+0x126a6) [0x7f520e5d66a6]
amf         | /lib/x86_64-linux-gnu/libpthread.so.0(+0x8609) [0x7f520dd4b609]
amf         | /lib/x86_64-linux-gnu/libc.so.6(clone+0x43) [0x7f520dc70133]
amf         | /open5gs_init.sh: line 96:    14 Aborted                 (core dumped) ./open5gs-amfd
amf exited with code 134
```

Upadate

We have reported this vulnerability to the vendor through email at 03 Aug 2022, but didn't get a reply.

The vendor pushed a commit at 05 Aug 2022, renaming the variable names from `gnb` to `peer` which didn't fix this vulnerability.

We confirmed that the latest version(2.4.10) is still affected by this vulnerability.

```
amf        | 09/15 09:45:22.032: [amf] INFO: [Added] Number of gNBs is now 125 (../src/amf/contex[36/1932]
amf        | 09/15 09:45:22.032: [amf] INFO: gNB-N2[10.10.94.173] max_num_of_ostreams : 10 (../src/amf/amf
-sm.c:698)
amf        | 09/15 09:45:22.033: [amf] WARNING: NG-Setup failure: (../src/amf/ngap-handler.c:305)
amf        | 09/15 09:45:22.033: [amf] WARNING:     Cannot find Served TAI. Check 'amf.tai' configuration
(../src/amf/ngap-handler.c:306)
amf        | 09/15 09:45:23.043: [amf] INFO: gNB-N2 accepted[10.10.94.173]:57205 in ng-path module (../src
/amf/ngap-sctp.c:113)
amf        | 09/15 09:45:23.043: [amf] INFO: gNB-N2 accepted[10.10.94.173] in master_sm module (../src/amf
/amf-sm.c:659)
amf        | 09/15 09:45:23.043: [amf] INFO: [Added] Number of gNBs is now 126 (../src/amf/context.c:880)
amf        | 09/15 09:45:23.043: [amf] INFO: gNB-N2[10.10.94.173] max_num_of_ostreams : 10 (../src/amf/amf
-sm.c:698)
amf        | 09/15 09:45:23.044: [amf] WARNING: NG-Setup failure: (../src/amf/ngap-handler.c:305)
amf        | 09/15 09:45:23.044: [amf] WARNING:     Cannot find Served TAI. Check 'amf.tai' configuration
(../src/amf/ngap-handler.c:306)
amf        | 09/15 09:45:24.041: [amf] INFO: gNB-N2 accepted[10.10.94.173]:48271 in ng-path module (../src
/amf/ngap-sctp.c:113)
amf        | 09/15 09:45:24.041: [amf] INFO: gNB-N2 accepted[10.10.94.173] in master_sm module (../src/amf
/amf-sm.c:659)
amf        | 09/15 09:45:24.041: [amf] INFO: [Added] Number of gNBs is now 127 (../src/amf/context.c:880)
amf        | 09/15 09:45:24.041: [amf] INFO: gNB-N2[10.10.94.173] max_num_of_ostreams : 10 (../src/amf/amf
-sm.c:698)
amf        | 09/15 09:45:24.042: [amf] WARNING: NG-Setup failure: (../src/amf/ngap-handler.c:305)
amf        | 09/15 09:45:24.042: [amf] WARNING:     Cannot find Served TAI. Check 'amf.tai' configuration
(../src/amf/ngap-handler.c:306)
amf        | 09/15 09:45:25.047: [amf] INFO: gNB-N2 accepted[10.10.94.173]:40959 in ng-path module (../src
/amf/ngap-sctp.c:113)
amf        | 09/15 09:45:25.047: [amf] INFO: gNB-N2 accepted[10.10.94.173] in master_sm module (../src/amf
/amf-sm.c:659)
amf        | 09/15 09:45:25.047: [amf] INFO: [Added] Number of gNBs is now 128 (../src/amf/context.c:880)
amf        | 09/15 09:45:25.047: [amf] INFO: gNB-N2[10.10.94.173] max_num_of_ostreams : 10 (../src/amf/amf
-sm.c:698)
amf        | 09/15 09:45:25.048: [amf] WARNING: NG-Setup failure: (../src/amf/ngap-handler.c:305)
amf        | 09/15 09:45:25.048: [amf] WARNING:     Cannot find Served TAI. Check 'amf.tai' configuration
(../src/amf/ngap-handler.c:306)
amf        | 09/15 09:45:26.048: [amf] INFO: gNB-N2 accepted[10.10.94.173]:49348 in ng-path module (../src
/amf/ngap-sctp.c:113)
amf        | 09/15 09:45:26.049: [amf] INFO: gNB-N2 accepted[10.10.94.173] in master_sm module (../src/amf
/amf-sm.c:659)
amf        | 09/15 09:45:26.049: [amf] FATAL: amf_gnb_add: Assertion `gnb' failed. (../src/amf/context.c:8
49)
amf        | 09/15 09:45:26.050: [core] FATAL: backtrace() returned 8 addresses (../lib/core/ogs-abort.c:3
7)
amf        | ./open5gs-amfd(+0xe33f) [0x56149149433f]
amf        | ./open5gs-amfd(+0x2f5a5) [0x5614914b55a5]
amf        | /open5gs/install/lib/x86_64-linux-gnu/libogscore.so.2(ogs_fsm_dispatch+0x113) [0x7fc97ac56417
]
amf        | ./open5gs-amfd(+0x8f64) [0x56149148ef64]
amf        | /open5gs/install/lib/x86_64-linux-gnu/libogscore.so.2(+0x117e5) [0x7fc97ac477e5]
amf        | /lib/x86_64-linux-gnu/libpthread.so.0(+0x8609) [0x7fc97a39e609]
amf        | /lib/x86_64-linux-gnu/libc.so.6(clone+0x43) [0x7fc97a2c3133]
amf        | /open5gs_init.sh: line 96:    14 Aborted                 (core dumped) ./open5gs-amfd
amf exited with code 134
```

CVE-2022-40890 had been assigned.

Acknowledgment

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

Releases

No releases published

Packages

No packages published