[Bugs] AMF breaks due to malformed NAS message #198

Open
p1-bmu opened this issue Apr 26, 2021 · 0 comments

p1-bmu commented Apr 26, 2021

...

Describe the bug

While testing the free5gc AMF for some NAS basic security features and fuzzing, I could trigger several crashes, while sending malformed NAS message. This means those issues are relatively exposed as they can be trigger by any 5G subscriber, in the principle.
Here, all memory issues due to mishandled NAS messages and IE structures are caught by the GO memory runtime, which protects the binary for potential exploitable cases.

To Reproduce

No easy way to reproduce with available open-source tools. A modification of a gNB / UE emulator can be done to send malformed NAS messages.

Expected behavior

An attacker could leverage this to cause excessive downtime and resource consumption against a pool of AMF. As much as possible, crashing the binary should be avoided when decoding subscriber's provided NAS signaling message. During the decoding process, verifications should be made to ensure the messages are valid ; in case of invalid or malformed messages, it should be dropped and the corresponding UE context should be deleted.

Environment (please complete the following information):

- free5GC Version: v3.0.5
- OS: Ubuntu 20.04
- Kernel version: 5.4.0-62-generic
- go version: go1.14.4 linux/amd64

Trace File

Configuration File

No specific configuration is required.

PCAP File

No specific pcap file is provided. If required, pcap corresponding some specific crashes can be provided.

Log File

The following part lists some GOLANG stacktraces and corresponding malformed NAS and IE cases.

When a IE with TLV structure (type 4 or 6) is provided, but without the expected length, free5gc crashes, e.g. with an empty 5GSID:

```
2021-03-08T12:18:12Z [INFO][AMF][GMM][AMF_UE_NGAP_ID:31] Handle Registration Request
panic: runtime error: index out of range [0] with length 0

goroutine 7 [running]:
github.com/free5gc/amf/gmm.HandleRegistrationRequest(0xc00011b080, 0xe3727a, 0xb, 0xf, 0xc0002cd790, 0xc0004e3530, 0xb75bb2)
        /home/p1sec/free5gc/NFs/amf/gmm/handler.go:425 +0x1969
github.com/free5gc/amf/gmm.DeRegistered(0xc0005a0600, 0xe373b9, 0xb, 0xc0005a0900)
        /home/p1sec/free5gc/NFs/amf/gmm/sm.go:30 +0x3ef
github.com/free5gc/fsm.(*FSM).SendEvent(0xc00009ab20, 0xc0005a0600, 0xe373b9, 0xb, 0xc0005a0900, 0x0, 0xcb6ba0)
        /home/p1sec/go/pkg/mod/github.com/free5gc/fsm@v1.0.0/fsm.go:95 +0x22d
github.com/free5gc/amf/nas.Dispatch(0xc00011b080, 0xe3727a, 0xb, 0xf, 0xc00047f980, 0x20, 0xc00047f980)
        /home/p1sec/free5gc/NFs/amf/nas/dispatch.go:22 +0x251
github.com/free5gc/amf/nas.HandleNAS(0xc0005d8a20, 0xf, 0xc000230f20, 0x11, 0x20)
        /home/p1sec/free5gc/NFs/amf/nas/handler.go:39 +0x178
github.com/free5gc/amf/ngap.HandleInitialUEMessage(0xc0005a4080, 0xc000248ce0)
        /home/p1sec/free5gc/NFs/amf/ngap/handler.go:1003 +0x4dc
github.com/free5gc/amf/ngap.Dispatch(0xfab8c0, 0xc00013fbe0, 0xc00029e000, 0x3c, 0x2000)
        /home/p1sec/free5gc/NFs/amf/ngap/dispatcher.go:47 +0x3bb
github.com/free5gc/amf/ngap/service.handleConnection(0xc00013fbe0, 0x2000, 0xe6a348, 0xe6a350)
        /home/p1sec/free5gc/NFs/amf/ngap/service/service.go:204 +0x700
created by github.com/free5gc/amf/ngap/service.listenAndServe
        /home/p1sec/free5gc/NFs/amf/ngap/service/service.go:136 +0xc43
```

Or a UE Security Capabilities:

```
panic: runtime error: index out of range [1] with length 0

goroutine 49 [running]:
github.com/free5gc/nas/nasType.(*UESecurityCapability).GetIA2_128_5G(...)
        /home/p1sec/go/pkg/mod/github.com/free5gc/nas@v1.0.0/nasType/NAS_UESecurityCapability.go:197
github.com/free5gc/amf/context.(*AmfUe).SelectSecurityAlg(0xc000118580, 0xc000385af8, 0x1, 0x8, 0xc000385b00, 0x1, 0x8)
        /home/p1sec/free5gc/NFs/amf/context/amf_ue.go:501 +0x226
github.com/free5gc/amf/gmm.SecurityMode(0xc00006f710, 0xe37356, 0xb, 0xc0003e7200)
        /home/p1sec/free5gc/NFs/amf/gmm/sm.go:221 +0xfb3
github.com/free5gc/fsm.(*FSM).SendEvent(0xc000386b50, 0xc00006f710, 0xe3efd6, 0x16, 0xc0003e7200, 0x0, 0x0)
        /home/p1sec/go/pkg/mod/github.com/free5gc/fsm@v1.0.0/fsm.go:100 +0x2f4
github.com/free5gc/amf/gmm.HandleAuthenticationResponse(0xc000118580, 0xe3727a, 0xb, 0xc0004e1b20, 0x1, 0x20)
        /home/p1sec/free5gc/NFs/amf/gmm/handler.go:1900 +0xdd8
github.com/free5gc/amf/gmm.Authentication(0xc00006f710, 0xe373b9, 0xb, 0xc0003e6390)
        /home/p1sec/free5gc/NFs/amf/gmm/sm.go:165 +0x5ce
github.com/free5gc/fsm.(*FSM).SendEvent(0xc000386b50, 0xc00006f710, 0xe373b9, 0xb, 0xc0003e6390, 0xc0004e1a60, 0xcb6ba0)
        /home/p1sec/go/pkg/mod/github.com/free5gc/fsm@v1.0.0/fsm.go:95 +0x22d
github.com/free5gc/amf/nas.Dispatch(0xc000118580, 0xe3727a, 0xb, 0x2e, 0xc0004e1b00, 0x20, 0xc0004e1b00)
        /home/p1sec/free5gc/NFs/amf/nas/dispatch.go:22 +0x251
github.com/free5gc/amf/nas.HandleNAS(0xc0003d3e60, 0x2e, 0xc00026e3c0, 0x15, 0x20)
        /home/p1sec/free5gc/NFs/amf/nas/handler.go:39 +0x178
github.com/free5gc/amf/ngap.HandleUplinkNasTransport(0xc000123e80, 0xc0004e09e0)
        /home/p1sec/free5gc/NFs/amf/ngap/handler.go:233 +0x701
github.com/free5gc/amf/ngap.Dispatch(0xfab8c0, 0xc000402120, 0xc0000c8000, 0x41, 0x2000)
        /home/p1sec/free5gc/NFs/amf/ngap/dispatcher.go:49 +0x527
github.com/free5gc/amf/ngap/service.handleConnection(0xc000402120, 0x2000, 0xe6a348, 0xe6a350)
        /home/p1sec/free5gc/NFs/amf/ngap/service/service.go:204 +0x700
created by github.com/free5gc/amf/ngap/service.listenAndServe
        /home/p1sec/free5gc/NFs/amf/ngap/service/service.go:136 +0xc43
```

This happens also with an oversized IE value, e.g. with 5G MM Capabilities:

```
2021-03-08T13:49:59Z [INFO][AMF][NGAP][172.27.128.253:38412] Handle Initial UE Message
panic: runtime error: slice bounds out of range [:32] with length 13

goroutine 7 [running]:
github.com/free5gc/nas/nasMessage.(*RegistrationRequest).DecodeRegistrationRequest(0xc000295e10, 0xc0001c1558)
        /home/p1sec/go/pkg/mod/github.com/free5gc/nas@v1.0.0/nasMessage/NAS_RegistrationRequest.go:195 +0x1b57
github.com/free5gc/nas.(*Message).GmmMessageDecode(0xc00047c0a0, 0xc0001c1558, 0x10000000000000b, 0xc0001c12d0)
        /home/p1sec/go/pkg/mod/github.com/free5gc/nas@v1.0.0/nas.go:201 +0x2de
github.com/free5gc/nas.(*Message).PlainNasDecode(0xc00047c0a0, 0xc0001c1558, 0xc0001c1510, 0x2)
        /home/p1sec/go/pkg/mod/github.com/free5gc/nas@v1.0.0/nas.go:175 +0x58
github.com/free5gc/amf/nas/nas_security.Decode(0xc0004ed600, 0xe3727a, 0xb, 0xc0003926c0, 0x3b, 0x40, 0x11, 0xc0004d4500, 0x
        /home/p1sec/free5gc/NFs/amf/nas/nas_security/security.go:136 +0x452
github.com/free5gc/amf/nas.HandleNAS(0xc000408240, 0xf, 0xc0003926c0, 0x3b, 0x40)
        /home/p1sec/free5gc/NFs/amf/nas/handler.go:33 +0xaa
github.com/free5gc/amf/ngap.HandleInitialUEMessage(0xc00030e180, 0xc000312ea0)
        /home/p1sec/free5gc/NFs/amf/ngap/handler.go:1003 +0x4dc
github.com/free5gc/amf/ngap.Dispatch(0xfab8c0, 0xc000277d70, 0xc0005f8000, 0x66, 0x2000)
        /home/p1sec/free5gc/NFs/amf/ngap/dispatcher.go:47 +0x3bb
github.com/free5gc/amf/ngap/service.handleConnection(0xc000277d70, 0x2000, 0xe6a348, 0xe6a350)
        /home/p1sec/free5gc/NFs/amf/ngap/service/service.go:204 +0x700
created by github.com/free5gc/amf/ngap/service.listenAndServe
        /home/p1sec/free5gc/NFs/amf/ngap/service/service.go:136 +0xc43
```

Providing malformed 5GSID can trigger several additional crashes in the `GutiToString` or `SuciToString` functions:

```
2021-03-08T12:22:45Z [INFO][AMF][GMM][AMF_UE_NGAP_ID:12] Handle Registration Request
panic: runtime error: slice bounds out of range [:4] with capacity 1

goroutine 7 [running]:
github.com/free5gc/nas/nasConvert.GutiToString(0xc000479530, 0x1, 0x1, 0xc000479530, 0x0, 0x0, 0x0, 0x0)
        /home/p1sec/go/pkg/mod/github.com/free5gc/nas@v1.0.0/nasConvert/MobileIdentity5GS.go:98 +0x386
github.com/free5gc/amf/gmm.HandleRegistrationRequest(0xc0005bb080, 0xe3727a, 0xb, 0xf, 0xc000351110, 0xc000743530, 0xb75bb2)
        /home/p1sec/free5gc/NFs/amf/gmm/handler.go:435 +0x111d
github.com/free5gc/amf/gmm.DeRegistered(0xc000452120, 0xe373b9, 0xb, 0xc0004526f0)
        /home/p1sec/free5gc/NFs/amf/gmm/sm.go:30 +0x3ef
github.com/free5gc/fsm.(*FSM).SendEvent(0xc000386ab0, 0xc000452120, 0xe373b9, 0xb, 0xc0004526f0, 0x0, 0xcb6ba0)
        /home/p1sec/go/pkg/mod/github.com/free5gc/fsm@v1.0.0/fsm.go:95 +0x22d
github.com/free5gc/amf/nas.Dispatch(0xc0005bb080, 0xe3727a, 0xb, 0xf, 0xc00000cca0, 0x20, 0xc00000cca0)
        /home/p1sec/free5gc/NFs/amf/nas/dispatch.go:22 +0x251
github.com/free5gc/amf/nas.HandleNAS(0xc0003d5e60, 0xf, 0xc0002e86c0, 0x12, 0x20)
        /home/p1sec/free5gc/NFs/amf/nas/handler.go:39 +0x178
github.com/free5gc/amf/ngap.HandleInitialUEMessage(0xc0000ca180, 0xc000316180)
        /home/p1sec/free5gc/NFs/amf/ngap/handler.go:1003 +0x4dc
github.com/free5gc/amf/ngap.Dispatch(0xfab8c0, 0xc00013fda0, 0xc0004d2000, 0x3d, 0x2000)
        /home/p1sec/free5gc/NFs/amf/ngap/dispatcher.go:47 +0x3bb
github.com/free5gc/amf/ngap/service.handleConnection(0xc00013fda0, 0x2000, 0xe6a348, 0xe6a350)
        /home/p1sec/free5gc/NFs/amf/ngap/service/service.go:204 +0x700
created by github.com/free5gc/amf/ngap/service.listenAndServe
        /home/p1sec/free5gc/NFs/amf/ngap/service/service.go:136 +0xc43
```

or

```
2021-03-08T12:27:02Z [INFO][AMF][GMM][AMF_UE_NGAP_ID:53] Handle Registration Request
panic: runtime error: index out of range [2] with length 1

goroutine 49 [running]:
github.com/free5gc/nas/nasConvert.SuciToString(0xc0002dcb20, 0x1, 0x1, 0xc0002dcb20, 0x0, 0x0, 0x0)
        /home/p1sec/go/pkg/mod/github.com/free5gc/nas@v1.0.0/nasConvert/MobileIdentity5GS.go:36 +0xaa9
github.com/free5gc/amf/gmm.HandleRegistrationRequest(0xc000113080, 0xe3727a, 0xb, 0xf, 0xc000281450, 0xc000075530, 0xb75bb2)
        /home/p1sec/free5gc/NFs/amf/gmm/handler.go:431 +0xd9c
github.com/free5gc/amf/gmm.DeRegistered(0xc000069f20, 0xe373b9, 0xb, 0xc0003d2780)
        /home/p1sec/free5gc/NFs/amf/gmm/sm.go:30 +0x3ef
github.com/free5gc/fsm.(*FSM).SendEvent(0xc000304b00, 0xc000069f20, 0xe373b9, 0xb, 0xc0003d2780, 0x0, 0xcb6ba0)
        /home/p1sec/go/pkg/mod/github.com/free5gc/fsm@v1.0.0/fsm.go:95 +0x22d
github.com/free5gc/amf/nas.Dispatch(0xc000113080, 0xe3727a, 0xb, 0xf, 0xc000628b60, 0x20, 0xc000628b60)
        /home/p1sec/free5gc/NFs/amf/nas/dispatch.go:22 +0x251
github.com/free5gc/amf/nas.HandleNAS(0xc0003de000, 0xf, 0xc000480240, 0x12, 0x20)
        /home/p1sec/free5gc/NFs/amf/nas/handler.go:39 +0x178
github.com/free5gc/amf/ngap.HandleInitialUEMessage(0xc0004c0180, 0xc0000981a0)
        /home/p1sec/free5gc/NFs/amf/ngap/handler.go:1003 +0x4dc
github.com/free5gc/amf/ngap.Dispatch(0xfab8c0, 0xc00009a140, 0xc00054e000, 0x3d, 0x2000)
        /home/p1sec/free5gc/NFs/amf/ngap/dispatcher.go:47 +0x3bb
github.com/free5gc/amf/ngap/service.handleConnection(0xc00009a140, 0x2000, 0xe6a348, 0xe6a350)
        /home/p1sec/free5gc/NFs/amf/ngap/service/service.go:204 +0x700
created by github.com/free5gc/amf/ngap/service.listenAndServe
        /home/p1sec/free5gc/NFs/amf/ngap/service/service.go:136 +0xc43
```

or

```
2021-03-08T13:29:29Z [INFO][AMF][GMM][AMF_UE_NGAP_ID:1] Handle Registration Request
panic: runtime error: index out of range [4] with length 4

goroutine 33 [running]:
github.com/free5gc/nas/nasConvert.SuciToString(0xc00054a588, 0x4, 0x4, 0xc00054a588, 0x0, 0x0, 0x0)
        /home/p1sec/go/pkg/mod/github.com/free5gc/nas@v1.0.0/nasConvert/MobileIdentity5GS.go:53 +0xa81
github.com/free5gc/amf/gmm.HandleRegistrationRequest(0xc00054e000, 0xe3727a, 0xb, 0xf, 0xc0005540d0, 0xc0004e5530, 0xb75bb2)
        /home/p1sec/free5gc/NFs/amf/gmm/handler.go:431 +0xd9c
github.com/free5gc/amf/gmm.DeRegistered(0xc00048cba0, 0xe373b9, 0xb, 0xc00048ced0)
        /home/p1sec/free5gc/NFs/amf/gmm/sm.go:30 +0x3ef
github.com/free5gc/fsm.(*FSM).SendEvent(0xc0002d6670, 0xc00048cba0, 0xe373b9, 0xb, 0xc00048ced0, 0x0, 0xcb6ba0)
        /home/p1sec/go/pkg/mod/github.com/free5gc/fsm@v1.0.0/fsm.go:95 +0x22d
github.com/free5gc/amf/nas.Dispatch(0xc00054e000, 0xe3727a, 0xb, 0xf, 0xc00053afa0, 0x20, 0xc00053afa0)
        /home/p1sec/free5gc/NFs/amf/nas/dispatch.go:22 +0x251
github.com/free5gc/amf/nas.HandleNAS(0xc0004c2240, 0xf, 0xc00049a940, 0x15, 0x20)
        /home/p1sec/free5gc/NFs/amf/nas/handler.go:39 +0x178
github.com/free5gc/amf/ngap.HandleInitialUEMessage(0xc0004b2000, 0xc000508880)
        /home/p1sec/free5gc/NFs/amf/ngap/handler.go:1003 +0x4dc
github.com/free5gc/amf/ngap.Dispatch(0xfab8c0, 0xc000304170, 0xc00051e000, 0x40, 0x2000)
        /home/p1sec/free5gc/NFs/amf/ngap/dispatcher.go:47 +0x3bb
github.com/free5gc/amf/ngap/service.handleConnection(0xc000304170, 0x2000, 0xe6a348, 0xe6a350)
        /home/p1sec/free5gc/NFs/amf/ngap/service/service.go:204 +0x700
created by github.com/free5gc/amf/ngap/service.listenAndServe
        /home/p1sec/free5gc/NFs/amf/ngap/service/service.go:136 +0xc43
```

Finally, it seems using any kind of LADN Indicator within the 5G Registration Request message leads to the AMF getting stuck, consuming CPU and memory forever, and not responding on the SCTP socket anymore. The process gets finally killed by the Linux kernel.
For instance sending a NAS Registration Request with the following LADN Indicator structure:

```
### LADNInd ###
 <T : 116>
 <L : 8>
 <V : 0x0000000000000000>
```

Leads to this situation:

```
[4410188.716481] Out of memory: Killed process 1955374 (amf) total-vm:19664848kB, anon-rss:7375620kB, file-rss:0kB, shmem-rs
[4410189.087583] oom_reaper: reaped process 1955374 (amf), now anon-rss:40kB, file-rss:0kB, shmem-rss:0kB
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant