New issue

Jump to bottom

[Bugs] A crafted malformed NGAP message can crash AMF and NGAP decoder #402

Open **fisherwky** opened this issue on Oct 14 · 4 comments

fisherwky commented on Oct 14

Describe the bug

A crafted malformed NGAP message can crash AMF and NGAP decoder

To Reproduce

run the program test.go can reproduce NGAP decoder crash:
fisher@ubuntu:~/free5gc/NFs/amf/internal/ngap$ cat test.go

```
package main

import (
        ngap "github.com/free5gc/ngap"
        "fmt"
)

func main() {
        data := []byte{0x00, 0x28, 0x00, 0x30, 0x00, 0x30, 0x30, 0x00, 0x12, 0x00, 0x20, 0x37,
0x37, 0x00, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30,
0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30,
0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30, 0x30}
        _, err := ngap.Decoder(data)
        fmt.Println(err)
}
```

fisher@ubuntu:~/free5gc/NFs/amf/internal/ngap$ go run test.go

```
panic: runtime error: index out of range [18446744073709551615] with length 29

goroutine 1 [running]:
```

```
github.com/free5gc/aper.GetBitString(0xc0000181e3, 0x1d, 0x1d, 0x0, 0x0, 0x4f3420, 0x6390c0,
0xc00007e6e0, 0x4b, 0x0)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:54 +0x2b2
github.com/free5gc/aper.GetBitsValue(0xc0000181e3, 0x1d, 0x1d, 0x0, 0x0, 0x0, 0x0, 0x0)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:83 +0x5a
github.com/free5gc/aper.(*perBitData).getBitsValue(0xc00009d140, 0x0, 0xc00009ba2f, 0x0, 0x0)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:117 +0x7a
github.com/free5gc/aper.(*perBitData).parseSemiConstrainedWholeNumber(0xc00009d140, 0x0, 0x1, 0x0,
0x0)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:191 +0x111
github.com/free5gc/aper.(*perBitData).parseNormallySmallNonNegativeWholeNumber(0xc00009d140,
0xc00001c140, 0x36, 0x1)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:204 +0x71
github.com/free5gc/aper.(*perBitData).parseEnumerated(0xc00009d140, 0x4f2b01, 0xc000015098,
0xc0000150a0, 0x1, 0xc0000164e0, 0x22)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:530 +0x168
github.com/free5gc/aper.parseField(0x4f2b60, 0xc000015080, 0x18b, 0xc00009d140, 0x10000, 0x0, 0x0,
0xc000015098, 0xc0000150a0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:727 +0x1a3e
github.com/free5gc/aper.parseField(0x507ca0, 0xc000015080, 0x199, 0xc00009d140, 0x1, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:853 +0x14ae
github.com/free5gc/aper.parseField(0x4da0c0, 0xc000078200, 0x196, 0xc00009d140, 0x1, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:686 +0x228f
github.com/free5gc/aper.parseField(0x538760, 0xc0000781c0, 0x199, 0xc00009d140, 0x10000, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:853 +0x14ae
github.com/free5gc/aper.parseField(0x4d70c0, 0xc000100050, 0x196, 0xc000089140, 0x10000, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:686 +0x228f
github.com/free5gc/aper.(*perBitData).parseOpenType(0xc00008acd0, 0x4d70c0, 0xc000100050, 0x196,
0x10000, 0x0, 0x0, 0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:668 +0x367
github.com/free5gc/aper.parseField(0x53db00, 0xc000100010, 0x199, 0xc00008acd0, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:805 +0xa99
github.com/free5gc/aper.parseField(0x52abe0, 0xc000100000, 0x199, 0xc00009ecd0, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:853 +0x14ae
github.com/free5gc/aper.(*perBitData).parseSequenceOf(0xc00009ecd0, 0x4ed800, 0x0, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:591 +0x347
github.com/free5gc/aper.parseField(0x4ed860, 0xc00000c7e0, 0x197, 0xc00008acd0, 0x0, 0xc0000149b0,
0xc0000149b8, 0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:860 +0x190d
github.com/free5gc/aper.parseField(0x5119a0, 0xc00000c7e0, 0x199, 0xc00009ecd0, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:853 +0x14ae
github.com/free5gc/aper.parseField(0x514e20, 0xc00000c7e0, 0x199, 0xc00009ecd0, 0x10000, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:853 +0x14ae
github.com/free5gc/aper.parseField(0x4e4480, 0xc000012408, 0x196, 0xc00008acd0, 0x10000, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:686 +0x228f
github.com/free5gc/aper.(*perBitData).parseOpenType(0xc00008be90, 0x4e4480, 0xc000012408, 0x196,
```

```
0x10000, 0x0, 0x0, 0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:668 +0x367
github.com/free5gc/aper.parseField(0x546a00, 0xc000012390, 0x199, 0xc00008be90, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:805 +0xa99
github.com/free5gc/aper.parseField(0x5236e0, 0xc000012380, 0x199, 0xc00009fe90, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:853 +0x14ae
github.com/free5gc/aper.parseField(0x4d9c80, 0xc00000c0e8, 0x196, 0xc000064e90, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:686 +0x228f
github.com/free5gc/aper.parseField(0x530d60, 0xc00000c0e0, 0x199, 0xc000064e90, 0x10000, 0x0, 0x0,
0xc0000140c0, 0xc0000140c8, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:819 +0xd9e
github.com/free5gc/aper.UnmarshalWithParams(0xc00001c0c0, 0x34, 0x34, 0x4da3c0, 0xc00000c0e0,
0x54bdd9, 0x1c, 0x0, 0x0)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:935 +0x1ce
github.com/free5gc/ngap.Decoder(...)
        /home/fisher/go/pkg/mod/github.com/free5gc/ngap@v1.0.6/ngap.go:19
main.main()
        /home/fisher/free5gc/NFs/amf/internal/ngap/test.go:10 +0xd7
exit status 2
```

When AMF receive this NGAP message will also crash

```
fisher@ubuntu:~/free5gc$ sudo ./bin/amf -c ./config/amfcfg.yaml -l ./log/20221014_091505/amf.log -
lc ./log/20221014_091505/free5gc.log
2022-10-14T09:28:34Z [INFO][AMF][CFG] config version [1.0.3]
2022-10-14T09:28:34Z [INFO][AMF][Init] AMF Log level is set to [info] level
2022-10-14T09:28:34Z [INFO][LIB][NAS] set log level : info
2022-10-14T09:28:34Z [INFO][LIB][NAS] set report call : false
2022-10-14T09:28:34Z [INFO][LIB][NGAP] set log level : info
2022-10-14T09:28:34Z [INFO][LIB][NGAP] set report call : false
2022-10-14T09:28:34Z [INFO][LIB][FSM] set log level : info
2022-10-14T09:28:34Z [INFO][LIB][FSM] set report call : false
2022-10-14T09:28:34Z [INFO][LIB][Aper] set log level : info
2022-10-14T09:28:34Z [INFO][LIB][Aper] set report call : false
2022-10-14T09:28:34Z [INFO][AMF][App] amf
2022-10-14T09:28:34Z [INFO][AMF][App] AMF version:
        free5GC version: v3.2.1-13-ge104d46
        build time:      2022-10-14T02:12:30Z
        commit hash:     e839de03
        commit time:     2022-08-25T12:35:10Z
        go version:      go1.14.4 linux/amd64
2022-10-14T09:28:34Z [INFO][AMF][Init] Server started
[GIN-debug] [WARNING] Running in "debug" mode. Switch to "release" mode in production.
 - using env:   export GIN_MODE=release
 - using code:  gin.SetMode(gin.ReleaseMode)

[GIN-debug] GET    /namf-callback/v1/        -->
github.com/free5gc/amf/internal/sbi/httpcallback.Index (4 handlers)
[GIN-debug] POST   /namf-callback/v1/smContextStatus/:guti/:pduSessionId -->
github.com/free5gc/amf/internal/sbi/httpcallback.HTTPSmContextStatusNotify (4 handlers)
[GIN-debug] POST   /namf-callback/v1/am-policy/:polAssoId/update -->
```

```
github.com/free5gc/amf/internal/sbi/httpcallback.HTTPAmPolicyControlUpdateNotifyUpdate (4
handlers)
[GIN-debug] POST   /namf-callback/v1/am-policy/:polAssoId/terminate -->
github.com/free5gc/amf/internal/sbi/httpcallback.HTTPAmPolicyControlUpdateNotifyTerminate (4
handlers)
[GIN-debug] POST   /namf-callback/v1/n1-message-notify -->
github.com/free5gc/amf/internal/sbi/httpcallback.HTTPN1MessageNotify (4 handlers)
[GIN-debug] GET    /namf-oam/v1/             --> github.com/free5gc/amf/internal/sbi/oam.Index (4
handlers)
[GIN-debug] GET    /namf-oam/v1/registered-ue-context -->
github.com/free5gc/amf/internal/sbi/oam.HTTPRegisteredUEContext (4 handlers)
[GIN-debug] GET    /namf-oam/v1/registered-ue-context/:supi -->
github.com/free5gc/amf/internal/sbi/oam.HTTPRegisteredUEContext (4 handlers)
[GIN-debug] GET    /namf-comm/v1/            -->
github.com/free5gc/amf/internal/sbi/communication.Index (4 handlers)
[GIN-debug] PUT    /namf-comm/v1/subscriptions/:subscriptionId -->
github.com/free5gc/amf/internal/sbi/communication.HTTPAMFStatusChangeSubscribeModify (4 handlers)
[GIN-debug] DELETE /namf-comm/v1/subscriptions/:subscriptionId -->
github.com/free5gc/amf/internal/sbi/communication.HTTPAMFStatusChangeUnSubscribe (4 handlers)
[GIN-debug] PUT    /namf-comm/v1/ue-contexts/:ueContextId -->
github.com/free5gc/amf/internal/sbi/communication.HTTPCreateUEContext (4 handlers)
[GIN-debug] POST   /namf-comm/v1/ue-contexts/:ueContextId/assign-ebi -->
github.com/free5gc/amf/internal/sbi/communication.HTTPEBIAssignment (4 handlers)
[GIN-debug] POST   /namf-comm/v1/ue-contexts/:ueContextId/transfer-update -->
github.com/free5gc/amf/internal/sbi/communication.HTTPRegistrationStatusUpdate (4 handlers)
[GIN-debug] POST   /namf-comm/v1/ue-contexts/:ueContextId/release -->
github.com/free5gc/amf/internal/sbi/communication.HTTPReleaseUEContext (4 handlers)
[GIN-debug] POST   /namf-comm/v1/ue-contexts/:ueContextId/transfer -->
github.com/free5gc/amf/internal/sbi/communication.HTTPUEContextTransfer (4 handlers)
[GIN-debug] DELETE /namf-comm/v1/ue-contexts/:ueContextId/n1-n2-
messages/subscriptions/:subscriptionId -->
github.com/free5gc/amf/internal/sbi/communication.HTTPN1N2MessageUnSubscribe (4 handlers)
[GIN-debug] POST   /namf-comm/v1/ue-contexts/:ueContextId/n1-n2-messages -->
github.com/free5gc/amf/internal/sbi/communication.HTTPN1N2MessageTransfer (4 handlers)
[GIN-debug] GET    /namf-comm/v1/ue-contexts/:ueContextId/n1-n2-messages/:n1N2MessageId -->
github.com/free5gc/amf/internal/sbi/communication.HTTPN1N2MessageTransferStatus (4 handlers)
[GIN-debug] POST   /namf-comm/v1/ue-contexts/:ueContextId/n1-n2-messages/subscriptions -->
github.com/free5gc/amf/internal/sbi/communication.HTTPN1N2MessageSubscribe (4 handlers)
[GIN-debug] DELETE /namf-comm/v1/non-ue-n2-messages/subscriptions/:n2NotifySubscriptionId -->
github.com/free5gc/amf/internal/sbi/communication.HTTPNonUeN2InfoUnSubscribe (4 handlers)
[GIN-debug] POST   /namf-comm/v1/non-ue-n2-messages/transfer -->
github.com/free5gc/amf/internal/sbi/communication.HTTPNonUeN2MessageTransfer (4 handlers)
[GIN-debug] POST   /namf-comm/v1/non-ue-n2-messages/subscriptions -->
github.com/free5gc/amf/internal/sbi/communication.HTTPNonUeN2InfoSubscribe (4 handlers)
[GIN-debug] POST   /namf-comm/v1/subscriptions -->
github.com/free5gc/amf/internal/sbi/communication.HTTPAMFStatusChangeSubscribe (4 handlers)
[GIN-debug] GET    /namf-evts/v1/            -->
github.com/free5gc/amf/internal/sbi/eventexposure.Index (4 handlers)
[GIN-debug] DELETE /namf-evts/v1/subscriptions/:subscriptionId -->
github.com/free5gc/amf/internal/sbi/eventexposure.HTTPDeleteSubscription (4 handlers)
[GIN-debug] PATCH  /namf-evts/v1/subscriptions/:subscriptionId -->
github.com/free5gc/amf/internal/sbi/eventexposure.HTTPModifySubscription (4 handlers)
[GIN-debug] POST   /namf-evts/v1/subscriptions -->
github.com/free5gc/amf/internal/sbi/eventexposure.HTTPCreateSubscription (4 handlers)
[GIN-debug] GET    /namf-mt/v1/              --> github.com/free5gc/amf/internal/sbi/mt.Index (4
handlers)
```

```
[GIN-debug] GET    /namf-mt/v1/ue-contexts/:ueContextId -->
github.com/free5gc/amf/internal/sbi/mt.HTTPProvideDomainSelectionInfo (4 handlers)
[GIN-debug] POST   /namf-mt/v1/ue-contexts/:ueContextId/ue-reachind -->
github.com/free5gc/amf/internal/sbi/mt.HTTPEnableUeReachability (4 handlers)
[GIN-debug] GET    /namf-loc/v1/             -->
github.com/free5gc/amf/internal/sbi/location.Index (4 handlers)
[GIN-debug] POST   /namf-loc/v1/:ueContextId/provide-loc-info -->
github.com/free5gc/amf/internal/sbi/location.HTTPProvideLocationInfo (4 handlers)
[GIN-debug] POST   /namf-loc/v1/:ueContextId/provide-pos-info -->
github.com/free5gc/amf/internal/sbi/location.HTTPProvidePositioningInfo (4 handlers)
2022-10-14T09:28:34Z [INFO][AMF][Util] amfconfig Info: Version[1.0.3] Description[AMF initial
local configuration]
2022-10-14T09:28:34Z [INFO][AMF][NGAP] Listen on 192.168.56.102:38412
2022-10-14T09:28:39Z [INFO][AMF][NGAP] [AMF] SCTP Accept from:
192.168.56.104/10.0.2.15/10.60.0.1/172.17.0.1:60710
2022-10-14T09:28:39Z [INFO][AMF][NGAP] Create a new NG connection for:
192.168.56.104/10.0.2.15/10.60.0.1/172.17.0.1:60710
panic: runtime error: index out of range [18446744073709551615] with length 29

goroutine 15 [running]:
github.com/free5gc/aper.GetBitString(0xc0003d7e23, 0x1d, 0x1d, 0x0, 0x0, 0xcef9e0, 0x16a0560,
0xc000029b80, 0x4b, 0x0)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:54 +0x2b2
github.com/free5gc/aper.GetBitsValue(0xc0003d7e23, 0x1d, 0x1d, 0x0, 0x0, 0x0, 0x0, 0x0)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:83 +0x5a
github.com/free5gc/aper.(*perBitData).getBitsValue(0xc000474f48, 0x0, 0xc000473837, 0x0, 0x0)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:117 +0x7a
github.com/free5gc/aper.(*perBitData).parseSemiConstrainedWholeNumber(0xc000474f48, 0x0, 0x1, 0x0,
0x0)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:191 +0x111
github.com/free5gc/aper.(*perBitData).parseNormallySmallNonNegativeWholeNumber(0xc000474f48,
0xc000452300, 0x36, 0x1)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:204 +0x71
github.com/free5gc/aper.(*perBitData).parseEnumerated(0xc000474f48, 0xcecf01, 0xc0004271e8,
0xc0004271f0, 0x1, 0xc00047a030, 0x22)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:530 +0x168
github.com/free5gc/aper.parseField(0xcecf20, 0xc0004271d0, 0x18b, 0xc000474f48, 0x10000, 0x0, 0x0,
0xc0004271e8, 0xc0004271f0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:727 +0x1a3e
github.com/free5gc/aper.parseField(0xd5b980, 0xc0004271d0, 0x199, 0xc000474f48, 0x1, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:853 +0x14ae
github.com/free5gc/aper.parseField(0xcadd80, 0xc0003dda80, 0x196, 0xc000474f48, 0x1, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:686 +0x228f
github.com/free5gc/aper.parseField(0xe00ec0, 0xc0003dda40, 0x199, 0xc000474f48, 0x10000, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:853 +0x14ae
github.com/free5gc/aper.parseField(0xcaad80, 0xc000480050, 0x196, 0xc0000a8f48, 0x10000, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:686 +0x228f
github.com/free5gc/aper.(*perBitData).parseOpenType(0xc0000aaad8, 0xcaad80, 0xc000480050, 0x196,
0x10000, 0x0, 0x0, 0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:668 +0x367
github.com/free5gc/aper.parseField(0xe25140, 0xc000480010, 0x199, 0xc0000aaad8, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
```

```
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:805 +0xa99
github.com/free5gc/aper.parseField(0xdb7600, 0xc000480000, 0x199, 0xc000476ad8, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:853 +0x14ae
github.com/free5gc/aper.(*perBitData).parseSequenceOf(0xc000476ad8, 0xcd9a00, 0x0, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:591 +0x347
github.com/free5gc/aper.parseField(0xcd9a60, 0xc0003f9020, 0x197, 0xc0000aaad8, 0x0, 0xc000426af0,
0xc000426af8, 0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:860 +0x190d
github.com/free5gc/aper.parseField(0xd65680, 0xc0003f9020, 0x199, 0xc000476ad8, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:853 +0x14ae
github.com/free5gc/aper.parseField(0xd68b00, 0xc0003f9020, 0x199, 0xc000476ad8, 0x10000, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:853 +0x14ae
github.com/free5gc/aper.parseField(0xcb8140, 0xc0000e5208, 0x196, 0xc0000aaad8, 0x10000, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:686 +0x228f
github.com/free5gc/aper.(*perBitData).parseOpenType(0xc0000abc98, 0xcb8140, 0xc0000e5208, 0x196,
0x10000, 0x0, 0x0, 0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:668 +0x367
github.com/free5gc/aper.parseField(0xe60ce0, 0xc0000e5190, 0x199, 0xc0000abc98, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:805 +0xa99
github.com/free5gc/aper.parseField(0xdb0100, 0xc0000e5180, 0x199, 0xc000477c98, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:853 +0x14ae
github.com/free5gc/aper.parseField(0xcad940, 0xc0003f8928, 0x196, 0xc00040bc98, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:686 +0x228f
github.com/free5gc/aper.parseField(0xddb1c0, 0xc0003f8920, 0x199, 0xc00040bc98, 0x10000, 0x0, 0x0,
0xc000426210, 0xc000426218, 0x0, ...)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:819 +0xd9e
github.com/free5gc/aper.UnmarshalWithParams(0xc000454000, 0x34, 0x2000, 0xcae080, 0xc0003f8920,
0xe882ed, 0x1c, 0xc0002f8ce0, 0x6)
        /home/fisher/go/pkg/mod/github.com/free5gc/aper@v1.0.4/aper.go:935 +0x1ce
github.com/free5gc/ngap.Decoder(...)
        /home/fisher/go/pkg/mod/github.com/free5gc/ngap@v1.0.6/ngap.go:19
github.com/free5gc/amf/internal/ngap.Dispatch(0x1000660, 0xc0004231f0, 0xc000454000, 0x34, 0x2000)
        /home/fisher/free5gc/NFs/amf/internal/ngap/dispatcher.go:30 +0x11a
github.com/free5gc/amf/internal/ngap/service.handleConnection(0xc0004231f0, 0x2000, 0xeaf6d8,
0xeaf6e0)
        /home/fisher/free5gc/NFs/amf/internal/ngap/service/service.go:204 +0x700
created by github.com/free5gc/amf/internal/ngap/service.listenAndServe
        /home/fisher/free5gc/NFs/amf/internal/ngap/service/service.go:136 +0xc43
```

Expected behavior

No crash of AMF and NGAP decoder

Environment (please complete the following information):

- free5GC Version: v3.2.1-13-ge104d46
- OS: Ubuntu 20.04 Server
- Kernel version: 5.4.0-91-generic
- go version: go1.14.4 linux/amd64
- c compiler version (Option): gcc (Ubuntu 9.4.0-1ubuntu1~20.04.1) 9.4.0

PCAP File

https://raw.githubusercontent.com/fisherwky/shared/main/crafted_malformed_ngap_message_make_amf_crash.pcap

CallmeprofessorD... commented 23 days ago

Hi,
May I ask how this loophole was dug?

fisherwky commented 23 days ago Author

> Hi, May I ask how this loophole was dug?

by fuzzing

CallmeprofessorD... commented 16 days ago

> Hi, May I ask how this loophole was dug?
>
> by fuzzing

Are open source tools used? If so, please tell me what it is. Thank you very much.

fisherwky commented 12 days ago Author

> > Hi, May I ask how this loophole was dug?
> >
> > by fuzzing
>
> Are open source tools used? If so, please tell me what it is. Thank you very much.

https://go.dev/security/fuzz/

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants