heap-buffer-overflow___libqasan_memset_libqasan.so+0x526c.spi

```
==================================================================
==14528==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f968fc368c8 at pc 0x7f97218161e4 bp 0x7f9723ffeb20 sp
0x7f9723ffead0
WRITE of size 1 at 0x7f968fc368c8 thread T14528
    #0 0x7f97218161e4 in __libqasan_memset /home/test/qasan/qasan/libqasan/string.c:68
    #1 0x7f9721814054 in memset /home/test/qasan/qasan/libqasan/hooks.c:248
    #2 0x7f97225f188c in maet_picbuf_alloc2 (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x6d88c)
    #3 0x7f97225d58c0 in maetd_dec (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x518c0)
    #4 0x7f97225d6ce0 in maetd_decode (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52ce0)
    #5 0x7f97225d3390 in _Z16read_maetel_argbPKN4SPen6StringEPiS3_S3_ (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x4f390)
    #6 0x7f972c676058 in _Z11ProcessFilePc (/home/test/notesfuzz/spiloader/spiloader+0x3058)
    #7 0x7f972c676190 in main (/home/test/notesfuzz/spiloader/spiloader+0x3190)
    #8 0x7f972176b0f4 in __libc_init (/home/test/samsung/system/lib64/libc.so+0xca0f4)
    #9 0x7f972c6751e0 in __atexit_handler_wrapper (/home/test/notesfuzz/spiloader/spiloader+0x21e0)
```

heap-buffer-overflow_maet_cpy_cb_libSPenBase.so+0x6b0d8.spi. ->

```
==14466==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f5a0845e100 at pc 0x7f5a8b0b33e0 bp 0x7f5a92fd2f20 sp
0x7f5a92fd2a40
READ of size 8 at 0x7f5a0845e100 thread T14466
    #0 0x7f5a8b0b33e0 in maet_cpy_cb (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x6d3e0)
    #1 0x7f5a8b097320 in maetd_pull_frm (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51320)
    #2 0x7f5a8b0984b4 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524b4)
    #3 0x7f5a8b098644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #4 0x7f5a8b098754 in maetd_dec_slice_mt (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52754)
    #5 0x7f5a8b097c18 in maetd_dec (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51c18)
    #6 0x7f5a8b098ce0 in maetd_decode (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52ce0)
    #7 0x7f5a8b095390 in _Z16read_maetel_argbPKN4SPen6StringEPiS3_S3_ (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x4f390)
    #8 0x7f5a972b6058 in _Z11ProcessFilePc (/home/test/notesfuzz/spiloader/spiloader+0x3058)
    #9 0x7f5a972b6190 in main (/home/test/notesfuzz/spiloader/spiloader+0x3190)
    #10 0x7f5a91cda0f4 in __libc_init (/home/test/samsung/system/lib64/libc.so+0xca0f4)
    #11 0x7f5a972b51e0 in __atexit_handler_wrapper (/home/test/notesfuzz/spiloader/spiloader+0x21e0)
```

heap-buffer-overflow_maet_get_pmv_libSPenBase.so+0x6a7c4.spi ->

```
==================================================================
==14410==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f1687759b9c at pc 0x7f170846cacc bp 0x7f1711e74f20 sp
0x7f1711e74a30
READ of size 4 at 0x7f1687759b9c thread T14410
    #0 0x7f170846cacc in maet_get_pmv (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x6cacc)
    #1 0x7f170845c4d0 in maetd_eco_nat (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5c4d0)
    #2 0x7f17084524fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
    #3 0x7f1708452644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #4 0x7f1708452754 in maetd_dec_slice_mt (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52754)
    #5 0x7f1708451c18 in maetd_dec (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51c18)
    #6 0x7f1708452ce0 in maetd_decode (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52ce0)
    #7 0x7f170844f390 in _Z16read_maetel_argbPKN4SPen6StringEPiS3_S3_ (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x4f390)
    #8 0x7f1716158058 in _Z11ProcessFilePc (/home/test/notesfuzz/spiloader/spiloader+0x3058)
    #9 0x7f1716158190 in main (/home/test/notesfuzz/spiloader/spiloader+0x3190)
    #10 0x7f170839c0f4 in __libc_init (/home/test/samsung/system/lib64/libc.so+0xca0f4)
    #11 0x7f17161571e0 in __atexit_handler_wrapper (/home/test/notesfuzz/spiloader/spiloader+0x21e0)
```

heap-buffer-overflow_maet_set_ipm_alpha_libSPenBase.so+0x6a790.spi

```
==================================================================
==14586==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f203c667c49 at pc 0x7f20c5a6da98 bp 0x7f203c501490 sp
0x7f203c501390
WRITE of size 1 at 0x7f203c667c49 thread T14589
    #0 0x7f20c5a6da98 in maet_set_ipm_alpha (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x6ca98)
    #1 0x7f20c5a5c944 in maetd_eco_raw_byte_a (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b944)
==================================================================
==14586==ERROR: QEMU-AddressSanitizer: heap-use-after-free on address 0x7f203c8100fc at pc 0x7f20c5a5c1f0 bp 0x7f203c5ff490 sp
0x7f203c5ff250
READ of size 1 at 0x7f203c8100fc thread T14588
    #2 0x7f20c5a534fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
==================================================================
==14586==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f203c63000a at pc 0x7f20c5a52fac bp 0x7f20c70daf20 sp
0x7f20c70daa50
WRITE of size 1 at 0x7f203c63000a thread T14586
    #0 0x7f20c5a5c1f0 in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b1f0)
    #3 0x7f20c5a53644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #0 0x7f20c5a52fac in maetd_flush (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51fac)
    #1 0x7f20c5a5c228 in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b228)
    #4 0x7f20c5a51bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #1 0x7f20c5a534b4 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524b4)
==================================================================
==14586==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f203c98114c at pc 0x7f20c5a5c08c bp 0x7f203c403490 sp
0x7f203c403250
WRITE of size 2 at 0x7f203c98114c thread T14590
    #2 0x7f20c5a5d610 in maetd_eco_nat (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5c610)
    #5 0x7f20bcd54c40 in _ZL15__pthread_startPv pthread_create.cpp:?
    #2 0x7f20c5a53644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #0 0x7f20c5a5c08c in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b08c)
    #3 0x7f20c5a534fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
    #6 0x7f20bcce7204 in __start_thread sfp-exceptions.c:?
```

heap-buffer-overflow_maet_set_ipm_libSPenBase.so+0x6a73c.spi

```
==14742==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7fc98163000c at pc 0x7fca06f95fac bp 0x7fc9815ff490 sp
0x7fc9815ff370
WRITE of size 1 at 0x7fc98163000c thread T14746
    #0 0x7fca06f95fac in maetd_flush (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51fac)
    #1 0x7fca06f964b4 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524b4)
    #2 0x7fca06f96644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #3 0x7fca06f94bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #4 0x7fca040edc40 in _ZL15__pthread_startPv pthread_create.cpp:?
==================================================================
==14742==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7fc98198114c at pc 0x7fca06f9f08c bp 0x7fc981501490 sp
0x7fc981501250
WRITE of size 2 at 0x7fc98198114c thread T14747
    #5 0x7fca04080204 in __start_thread sfp-exceptions.c:?
0x7fc98163000c is located 84 bytes to the left of 128-byte region [0x7fc981630060,0x7fc9816300e0)
freed by thread T14742 here:
    #0 0x7fca06f9f08c in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b08c)
    #0 0x7fca0407b330 in syscall (/home/test/samsung/system/lib64/libc.so+0x1f330)
    #1 0x7fca06f9f540 in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b540)
    #1 0x7fca050c5930 in __libqasan_free /home/test/qasan/qasan/libqasan/malloc.c:220
    #2 0x7fca06fa0610 in maetd_eco_nat (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5c610)
```

```
    #2 0x7fca050c3d40 in free /home/test/qasan/qasan/libqasan/hooks.c:169
    #3 0x7fca06f964fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
    #3 0x7fca0422f1b8 in _ZNSt3__113__tree_removeIPNS_16__tree_node_baseIPvEEEEvT_S5_
(/home/test/samsung/system/lib64/libhidltransport.so+0x2a1b8)
    #4 0x7fca06f96644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #4 0x7fca04236188 in
_ZNSt3__16__treeINS_12__value_typeINS_12basic_stringIcNS_11char_traitsIcEENS_9allocatorIcEEEEENS_8functionIFN7android2spINS9_8hardware7IBinderE
(/home/test/samsung/system/lib64/libhidltransport.so+0x31188)
    #5 0x7fca06f94bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #5 0x7fca04235e84 in
_ZNSt3__113__vector_baseINS_4pairIN7android4hidl4base4V1_09DebugInfo12ArchitectureENS_6vectorIPKcNS_9allocatorISA_EEEEEENSB_ISE_EEED2Ev
(/home/test/samsung/system/lib64/libhidltransport.so+0x30e84)
    #6 0x7fca040edc40 in _ZL15__pthread_startPv pthread_create.cpp:?
    #6 0x7fca05c959c4 in _ZN7android6FQName5setToERKNSt3__112basi
```

heap-buffer-overflow_maetd_dec_libSPenBase.so+0x4f40c.spi

```
➜  newnote AFL_INST_LIBS=1 LD_LIBRARY_PATH=$ANDROID_NDK/toolchains/llvm/prebuilt/linux-x86_64/sysroot/usr/lib/aarch64-linux-
android:$ANDROID_PATH/lib64:$APPLIB_PATH ~/qasan/qasan/qasan ~/notesfuzz/spiloader/spiloader -f /tmp/triaged_spi/heap-buffer-
overflow_maetd_dec_libSPenBase.so+0x4f40c.spi
=================================================================
==14875==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f5f06847d20 at pc 0x7f5f87292718 bp 0x7f5f91369f20 sp
0x7f5f91369ba0
WRITE of size 8 at 0x7f5f06847d20 thread T14875
    #0 0x7f5f87292718 in maetd_dec (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51718)
    #1 0x7f5f87293ce0 in maetd_decode (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52ce0)
    #2 0x7f5f87290390 in _Z16read_maetel_argbPKN4SPen6StringEPiS3_S3_ (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x4f390)
    #3 0x7f5f9564d058 in _Z11ProcessFilePc (/home/test/notesfuzz/spiloader/spiloader+0x3058)
    #4 0x7f5f9564d190 in main (/home/test/notesfuzz/spiloader/spiloader+0x3190)
    #5 0x7f5f88cd90f4 in __libc_init (/home/test/samsung/system/lib64/libc.so+0xca0f4)
    #6 0x7f5f9564c1e0 in __atexit_handler_wrapper (/home/test/notesfuzz/spiloader/spiloader+0x21e0)
0x7f5f06847d20 is located 0 bytes to the left of 0-byte region [0x7f5f06847d20,0x7f5f06847d20)
allocated by thread T14875 here:
    #0 0x7f5f88c2e330 in syscall (/home/test/samsung/system/lib64/libc.so+0x1f330)
    #1 0x7f5f88d64668 in __libqasan_malloc /home/test/qasan/qasan/libqasan/malloc.c:173
    #2 0x7f5f88d62ae0 in malloc /home/test/qasan/qasan/libqasan/hooks.c:68
    #3 0x7f5f8729289c in maetd_dec (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5189c)
    #4 0x7f5f87293ce0 in maetd_decode (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52ce0)
    #5 0x7f5f87290390 in _Z16read_maetel_argbPKN4SPen6StringEPiS3_S3_ (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x4f390)
    #6 0x7f5f9564d058 in _Z11ProcessFilePc (/home/test/notesfuzz/spiloader/spiloader+0x3058)
    #7 0x7f5f9564d190 in main (/home/test/notesfuzz/spiloader/spiloader+0x3190)
    #8 0x7f5f88cd90f4 in __libc_init (/home/test/samsung/system/lib64/libc.so+0xca0f4)
    #9 0x7f5f9564c1e0 in __atexit_handler_wrapper (/home/test/notesfuzz/spiloader/spiloader+0x21e0)
SUMMARY: QEMU-AddressSanitizer: heap-buffer-overflow in maetd_dec (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51718)
```

heap-buffer-overflow_maetd_eco_cb_syn_libSPenBase.so+0x5b17c.spi

```
=================================================================
==14924==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f620fd59b88 at pc 0x7f6293a1e488 bp 0x7f629a55ef20 sp
0x7f629a55e9d0
WRITE of size 1 at 0x7f620fd59b88 thread T14924
=================================================================
==14924==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f620fa3002f at pc 0x7f6293a12fac bp 0x7f620f9ff490 sp
0x7f620f9ff370
WRITE of size 1 at 0x7f620fa3002f thread T14927
=================================================================
==14924==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f620fa40033 at pc 0x7f6293a12fac bp 0x7f620f901490 sp
0x7f620f901370
WRITE of size 1 at 0x7f620fa40033 thread T14928
    #0 0x7f6293a1e488 in maetd_eco_cb_syn (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5d488)
    #0 0x7f6293a12fac in maetd_flush (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51fac)
    #0 0x7f6293a12fac in maetd_flush (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51fac)
    #1 0x7f6293a1e874 in maetd_eco_pcm_idx (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5d874)
    #1 0x7f6293a134b4 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524b4)
    #1 0x7f6293a134b4 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524b4)
    #2 0x7f6293a134fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
    #2 0x7f6293a13644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #2 0x7f6293a13644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #3 0x7f6293a13644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #3 0x7f6293a11bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #3 0x7f6293a11bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #4 0x7f6293a13754 in maetd_dec_slice_mt (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52754)
    #4 0x7f6291799c40 in _ZL15__pthread_startPv pthread_create.cpp:?
    #4 0x7f6291799c40 in _ZL15__pthread_startPv pthread_create.cpp:?
    #5 0x7f6293a12c18 in maetd_dec (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51c18)
    #5 0x7f629172c204 in __start_thread sfp-exceptions.c:?
```

heap-buffer-overflow_maetd_eco_cb_syn_libSPenBase.so+0x5b19c.spi

```
=================================================================
==15074==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f1971d59b88 at pc 0x7f19f59a14a8 bp 0x7f19f7ffef20 sp
0x7f19f7ffe9d0
WRITE of size 1 at 0x7f1971d59b88 thread T15074
    #0 0x7f19f59a14a8 in maetd_eco_cb_syn (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5d4a8)
    #1 0x7f19f59a1874 in maetd_eco_pcm_idx (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5d874)
    #2 0x7f19f59964fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
    #3 0x7f19f5996644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #4 0x7f19f5996754 in maetd_dec_slice_mt (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52754)
=================================================================
==15074==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f1971d8114c at pc 0x7f19f599f08c bp 0x7f1971803490 sp
0x7f1971803250
WRITE of size 2 at 0x7f1971d8114c thread T15078
    #5 0x7f19f5995c18 in maetd_dec (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51c18)
    #0 0x7f19f599f08c in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b08c)
    #6 0x7f19f5996ce0 in maetd_decode (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52ce0)
    #1 0x7f19f599f540 in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b540)
    #7 0x7f19f5993560 in _Z16read_maetel_argbPKN4SPen6StringEPiS3_S3_ (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x4f560)
    #2 0x7f19f59a0610 in maetd_eco_nat (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5c610)
    #8 0x7f1a0079f058 in _Z11ProcessFilePc (/home/test/notesfuzz/spiloader/spiloader+0x3058)
    #3 0x7f19f59964fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
    #9 0x7f1a0079f190 in main (/home/test/notesfuzz/spiloader/spiloader+0x3190)
    #4 0x7f19f5996644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #10 0x7f19f73cd0f4 in __libc_init (/home/test/samsung/system/lib64/libc.so+0xca0f4)
    #5 0x7f19f5994bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #11 0x7f1a0079e1e0 in __atexit_handler_wrapper (/home/test/notesfuzz/spiloader/spiloader+0x21e0)
```

heap-buffer-overflow_maetd_eco_intra_nat_libSPenBase.so+0x59d10.spi

```
==15174==ERROR: QEMU-AddressSanitizer: heap-use-after-free on address 0x7fda466102f9 at pc 0x7fdac92e101c bp 0x7fdad1000f20 sp
0x7fdad1000980
READ of size 1 at 0x7fda466102f9 thread T15174
    #0 0x7fdac92e101c in maetd_eco_intra_nat (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5c01c)
    #1 0x7fdac92e0fe8 in maetd_eco_intra_nat (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5bfe8)
    #2 0x7fdac92e1e94 in maetd_eco_nat (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5ce94)
    #3 0x7fdac92d74fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
    #4 0x7fdac92d7644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #5 0x7fdac92d7754 in maetd_dec_slice_mt (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52754)
    #6 0x7fdac92d6c18 in maetd_dec (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51c18)
    #7 0x7fdac92d7ce0 in maetd_decode (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52ce0)
    #8 0x7fdac92d4560 in _Z16read_maetel_argbPKN4SPen6StringEPiS3_S3_ (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x4f560)
```

```
    #9 0x7fdad52e4058 in _Z11ProcessFilePc (/home/test/notesfuzz/spiloader/spiloader+0x3058)
    #10 0x7fdad52e4190 in main (/home/test/notesfuzz/spiloader/spiloader+0x3190)
    #11 0x7fdac87a00f4 in __libc_init (/home/test/samsung/system/lib64/libc.so+0xca0f4)
    #12 0x7fdad52e31e0 in __atexit_handler_wrapper (/home/test/notesfuzz/spiloader/spiloader+0x21e0)
0x7fda466102f9 is located 5721 bytes inside of 6376-byte region [0x7fda4660eca0,0x7fda46610588)
freed by thread T15174 here:
    #0 0x7fdac86f5330 in syscall (/home/test/samsung/system/lib64/libc.so+0x1f330)
    #1 0x7fdacb68b930 in __libqasan_free /home/test/qasan/qasan/libqasan/malloc.c:220
    #2 0x7fdacb689d40 in free /home/test/qasan/qasan/libqasan/hooks.c:169
    #3 0x7fdac832a680 in _ZNK7android12SortedVectorINS_16key_value_pair_tINS_8String16ES2_EEE10do_compareEPKvS6_
(/home/test/samsung/system/lib64/libandroidfw.so+0x2a680)
    #4 0x7fdac8332008 in _ZN7android10LoadedArsc4LoadERKNS_16BasicStringPieceIcEEPKNS_11LoadedIdmapEbb
(/home/test/samsung/system/lib64/libandroidfw.so+0x32008)
    #5 0x7fdac831a2a4 (/home/test/samsung/system/lib64/libandroidfw.so+0x1a2a4)
    #6 0x7fdad06c4ca4 in __dl__ZL10call_arrayIPFviPPcS1_EEvPKcPT_mbS5_ __dl_linker_soinfo.cpp:?
    #7 0x7fdad06c4fd8 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #8 0x7fdad06c4ee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #9 0x7fdad06c4ee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #10 0x7fdad06c4ee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #11 0x7fdad06c4ee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #12 0x7fdad06c4ee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #13 0x7fdad06c4ee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #14 0x7fdad06c0c04 in __dl___linker_init __dl_ubsan_minimal_handlers.cc:?
    #15 0x7fdad06c7478 in __dl__start __dl_ubsan_minimal_handlers.cc:?
```

heap-buffer-overflow_maetd_eco_skip_ext_libSPenBase.so+0x58d80.spi

```
==15278==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7fefa37811b8 at pc 0x7ff02706108c bp 0x7fefa3203490 sp
0x7fefa3203250
WRITE of size 2 at 0x7fefa37811b8 thread T15282
    #0 0x7ff02706108c in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b08c)
    #1 0x7ff027061540 in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b540)
    #2 0x7ff027062610 in maetd_eco_nat (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5c610)
    #3 0x7ff0270584fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
    #4 0x7ff027058644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #5 0x7ff027056bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #6 0x7ff027bebc40 in _ZL15__pthread_startPv pthread_create.cpp:?
    #7 0x7ff027b7e204 in __start_thread sfp-exceptions.c:?
```

heap-buffer-overflow_maetd_eco_skip_ext_libSPenBase.so+0x58e4c.spi

```
==================================================================
==15342==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7ff399981174 at pc 0x7ff41e9a008c bp 0x7ff399403490 sp
0x7ff399403250
WRITE of size 2 at 0x7ff399981174 thread T15346
    #0 0x7ff41e9a008c in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b08c)
    #1 0x7ff41e9a0540 in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b540)
    #2 0x7ff41e9a1610 in maetd_eco_nat (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5c610)
    #3 0x7ff41e9974fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
    #4 0x7ff41e997644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #5 0x7ff41e995bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #6 0x7ff41eb29c40 in _ZL15__pthread_startPv pthread_create.cpp:?
    #7 0x7ff41eabc204 in __start_thread sfp-exceptions.c:?
```

heap-buffer-overflow_maetd_eco_skip_ext_libSPenBase.so+0x58ee4.spi

```
==15403==ERROR: QEMU-AddressSanitizer: heap-use-after-free on address 0x7f7c7c610003 at pc 0x7f7cfea5f1f0 bp 0x7f7c7c3ff490 sp
0x7f7c7c3ff250
READ of size 1 at 0x7f7c7c610003 thread T15405
==================================================================
==15403==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f7c7c7769dc at pc 0x7f7cfea5f158 bp 0x7f7c7c301490 sp
0x7f7c7c301250
WRITE of size 2 at 0x7f7c7c7769dc thread T15406
    #0 0x7f7cfea5f1f0 in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b1f0)
    #0 0x7f7cfea5f158 in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b158)
    #1 0x7f7cfea5f228 in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b228)
    #1 0x7f7cfea5f540 in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b540)
    #2 0x7f7cfea60610 in maetd_eco_nat (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5c610)
    #2 0x7f7cfea60610 in maetd_eco_nat (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5c610)
    #3 0x7f7cfea564fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
    #3 0x7f7cfea564fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
    #4 0x7f7cfea56644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #4 0x7f7cfea56644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #5 0x7f7cfea54bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #5 0x7f7cfea54bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #6 0x7f7d05830c40 in _ZL15__pthread_startPv pthread_create.cpp:?
    #6 0x7f7d05830c40 in _ZL15__pthread_startPv pthread_create.cpp:?
    #7 0x7f7d057c3204 in __start_thread sfp-exceptions.c:?
```

heap-buffer-overflow_maetd_eco_skip_ext_libSPenBase.so+0x590e4.spi

```
==15519==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f53c4d7d9b8 at pc 0x7f54466de3f0 bp 0x7f53c49ff490 sp
0x7f53c49ff260
WRITE of size 2 at 0x7f53c4d7d9b8 thread T15522
    #0 0x7f54466de3f0 in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b3f0)
    #1 0x7f54466de5b0 in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b5b0)
    #2 0x7f54466dfcd8 in maetd_eco_nat (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5ccd8)
    #3 0x7f54466e0290 in maetd_eco_pred_block_a (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5d290)
    #4 0x7f54466d54fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
    #5 0x7f54466d5644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #6 0x7f54466d3bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #7 0x7f544deadc40 in _ZL15__pthread_startPv pthread_create.cpp:?
    #8 0x7f544de40204 in __start_thread sfp-exceptions.c:?
0x7f53c4d7d9b8 is located 40 bytes to the left of 24-byte region [0x7f53c4d7d9e0,0x7f53c4d7d9f8)
allocated by thread T15519 here:
    #0 0x7f544de3b330 in syscall (/home/test/samsung/system/lib64/libc.so+0x1f330)
    #1 0x7f544738a668 in __libqasan_malloc /home/test/qasan/qasan/libqasan/malloc.c:173
    #2 0x7f5447388ae0 in malloc /home/test/qasan/qasan/libqasan/hooks.c:68
    #3 0x7f5446597c48 in _ZNSt20bad_array_new_lengthD0Ev (/home/test/samsung/system/lib64/libc++.so+0x50c48)
    #4 0x7f54454f1fa4 in _ZN7android10LoadedArsc4LoadERKNS_16BasicStringPieceIcEEPKNS_11LoadedIdmapEbb
(/home/test/samsung/system/lib64/libandroidfw.so+0x31fa4)
    #5 0x7f54454da2a4 (/home/test/samsung/system/lib64/libandroidfw.so+0x1a2a4)
    #6 0x7f544ecbeca4 in __dl__ZL10call_arrayIPFviPPcS1_EEvPKcPT_mbS5_ __dl_linker_soinfo.cpp:?
    #7 0x7f544ecbefd8 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #8 0x7f544ecbeee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #9 0x7f544ecbeee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #10 0x7f544ecbeee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #11 0x7f544ecbeee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
==================================================================
==15519==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f53c4a60099 at pc 0x7f54466efa44 bp 0x7f53c4901490 sp
0x7f53c49013a0
WRITE of size 1 at 0x7f53c4a60099 thread T15523
    #12 0x7f544ecbeee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #0 0x7f54466efa44 in maet_set_ipm (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x6ca44)
    #13 0x7f544ecbeee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #1 0x7f54466dd41c in maetd_eco_skip (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5a41c)
    #14 0x7f544ecbac04 in __dl___linker_init __dl_ubsan_minimal_handlers.cc:?
    #2 0x7f54466d54fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
    #3 0x7f54466d5644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
```

```
    #15 0x7f544ecc1478 in __dl__start __dl_ubsan_minimal_handlers.cc:?
```

heap-buffer-overflow_maetd_eco_skip_ext_libSPenBase.so+0x591cc.spi

```
==15591==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f4b0e56f94c at pc 0x7f4b8fc9d4d8 bp 0x7f4b98daef20 sp
0x7f4b98dae940
WRITE of size 2 at 0x7f4b0e56f94c thread T15591
    #0 0x7f4b8fc9d4d8 in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b4d8)
    #1 0x7f4b8fc9d5b0 in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b5b0)
    #2 0x7f4b8fc9e954 in maetd_eco_nat (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5c954)
    #3 0x7f4b8fc9f290 in maetd_eco_pred_block_a (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5d290)
    #4 0x7f4b8fc944fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
    #5 0x7f4b8fc94644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #6 0x7f4b8fc94754 in maetd_dec_slice_mt (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52754)
    #7 0x7f4b8fc93c18 in maetd_dec (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51c18)
    #8 0x7f4b8fc94ce0 in maetd_decode (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52ce0)
    #9 0x7f4b8fc91560 in _Z16read_maetel_argbPKN4SPen6StringEPiS3_S3_ (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x4f560)
    #10 0x7f4b9d092058 in _Z11ProcessFilePc (/home/test/notesfuzz/spiloader/spiloader+0x3058)
    #11 0x7f4b9d092190 in main (/home/test/notesfuzz/spiloader/spiloader+0x3190)
    #12 0x7f4b9100e0f4 in __libc_init (/home/test/samsung/system/lib64/libc.so+0xca0f4)
    #13 0x7f4b9d0911e0 in __atexit_handler_wrapper (/home/test/notesfuzz/spiloader/spiloader+0x21e0)
0x7f4b0e56f94c is located 20 bytes to the left of 24-byte region [0x7f4b0e56f960,0x7f4b0e56f978)
allocated by thread T15591 here:
    #0 0x7f4b90f63330 in syscall (/home/test/samsung/system/lib64/libc.so+0x1f330)
    #1 0x7f4b92159668 in __libqasan_malloc /home/test/qasan/qasan/libqasan/malloc.c:173
    #2 0x7f4b92157ae0 in malloc /home/test/qasan/qasan/libqasan/hooks.c:68
    #3 0x7f4b91d51c48 in _ZNSt20bad_array_new_lengthD0Ev (/home/test/samsung/system/lib64/libc++.so+0x50c48)
    #4 0x7f4b8fdb1fa4 in _ZN7android10LoadedArsc4LoadERKNS_16BasicStringPieceIcEEPKNS_11LoadedIdmapEbb
(/home/test/samsung/system/lib64/libandroidfw.so+0x31fa4)
    #5 0x7f4b8fd9a2a4 (/home/test/samsung/system/lib64/libandroidfw.so+0x1a2a4)
    #6 0x7f4b98472ca4 in __dl__ZL10call_arrayIPFviPPcS1_EEvPKcPT_mbS5_ __dl_linker_soinfo.cpp:?
    #7 0x7f4b98472fd8 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #8 0x7f4b98472ee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #9 0x7f4b98472ee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #10 0x7f4b98472ee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #11 0x7f4b98472ee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #12 0x7f4b98472ee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #13 0x7f4b98472ee4 in __dl__ZN6soinfo17call_constructorsEv __dl_ubsan_minimal_handlers.cc:?
    #14 0x7f4b9846ec04 in __dl___linker_init __dl_ubsan_minimal_handlers.cc:?
    #15 0x7f4b98475478 in __dl__start __dl_ubsan_minimal_handlers.cc:?
```

heap-buffer-overflow_maetd_eco_skip_libSPenBase.so+0x58d80c.spi

```
==15667==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7fa7d0d7a1b8 at pc 0x7fa853f9e08c bp 0x7fa7d0803490 sp
0x7fa7d0803250
WRITE of size 2 at 0x7fa7d0d7a1b8 thread T15671
    #0 0x7fa853f9e08c in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b08c)
    #1 0x7fa853f9e540 in maetd_eco_skip_ext (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5b540)
    #2 0x7fa853f9f610 in maetd_eco_nat (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5c610)
    #3 0x7fa853f954fc in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524fc)
    #4 0x7fa853f95644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #5 0x7fa853f93bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #6 0x7fa851d2ec40 in _ZL15__pthread_startPv pthread_create.cpp:?
    #7 0x7fa851cc1204 in __start_thread sfp-exceptions.c:?
```

heap-buffer-overflow_maetd_flush_libSPenBase.so+0x4fca0.spi

```
==15727==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f7310c3002e at pc 0x7f7393cd7fac bp 0x7f7310a03490 sp
0x7f7310a03370
WRITE of size 1 at 0x7f7310c3002e thread T15731
    #0 0x7f7393cd7fac in maetd_flush (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51fac)
    #1 0x7f7393cd84b4 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524b4)
    #2 0x7f7393cd8644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #3 0x7f7393cd6bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #4 0x7f7393a65c40 in _ZL15__pthread_startPv pthread_create.cpp:?
    #5 0x7f73939f8204 in __start_thread sfp-exceptions.c:?
```

heap-buffer-overflow_maetd_flush_libSPenBase.so+0x4fde4.spi

```
=================================================================
==15821==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f8fac230001 at pc 0x7f9035456f0 bp 0x7f8fac1ff490 sp
0x7f8fac1ff370
WRITE of size 1 at 0x7f8fac230001 thread T15823
=================================================================
==15821==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f8fac240001 at pc 0x7f9035455fac bp 0x7f8fac101490 sp
0x7f8fac101370
WRITE of size 1 at 0x7f8fac240001 thread T15824
=================================================================
==15821==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f8fac240005 at pc 0x7f9035455fac bp 0x7f8fa7fff490 sp
0x7f8fa7fff370
WRITE of size 1 at 0x7f8fac240005 thread T15825
=================================================================
==15821==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7f8fac230028 at pc 0x7f9035455fac bp 0x7f9036c42f20 sp
0x7f9036c42a50
WRITE of size 1 at 0x7f8fac230028 thread T15821
    #0 0x7f90354560f0 in maetd_flush (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x520f0)
    #0 0x7f9035455fac in maetd_flush (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51fac)
    #0 0x7f9035455fac in maetd_flush (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51fac)
    #0 0x7f9035455fac in maetd_flush (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51fac)
    #1 0x7f90354564b4 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524b4)
    #1 0x7f90354564b4 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524b4)
    #1 0x7f90354564b4 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524b4)
    #1 0x7f90354564b4 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x524b4)
    #2 0x7f9035456644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #2 0x7f9035456644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #2 0x7f9035456644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #2 0x7f9035456644 in maetd_dec_slice (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52644)
    #3 0x7f9035454bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #3 0x7f9035454bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #3 0x7f9035454bc4 in _Z17write_maetel_argbPKN4SPen6StringEPhjjji (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x50bc4)
    #3 0x7f9035456754 in maetd_dec_slice_mt (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52754)
    #4 0x7f90347eac40 in _ZL15__pthread_startPv pthread_create.cpp:?
    #4 0x7f90347eac40 in _ZL15__pthread_startPv pthread_create.cpp:?
    #4 0x7f90347eac40 in _ZL15__pthread_startPv pthread_create.cpp:?
    #4 0x7f9035455c18 in maetd_dec (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51c18)
    #5 0x7f903477d204 in __start_thread sfp-exceptions.c:?
```

heap-buffer-overflow_syscall_libc.so+0x1f330.spi

```
➜  newnote AFL_INST_LIBS=1 LD_LIBRARY_PATH=$ANDROID_NDK/toolchains/llvm/prebuilt/linux-x86_64/sysroot/usr/lib/aarch64-linux-
android:$ANDROID_PATH/lib64:$APPLIB_PATH ~/qasan/qasan/qasan ~/notesfuzz/spiloader/spiloader -f /tmp/triaged_spi/heap-buffer-
overflow_syscall_libc.so+0x1f330.spi
=================================================================
==16040==ERROR: QEMU-AddressSanitizer: heap-buffer-overflow on address 0x7fe96c0383c3 at pc 0x7fe9ed4c3330 bp 0x7fe9f69c6870 sp
0x7fe9f69c6840
WRITE of size 13 at 0x7fe96c0383c3 thread T16040
    #0 0x7fe9ed4c3330 in syscall (/home/test/samsung/system/lib64/libc.so+0x1f330)
    #1 0x7fe9f538e038 in memset /home/test/qasan/qasan/libqasan/hooks.c:248
```

```
    #2 0x7fe9f52bcf30 in sxqk_imgb_option (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x7bf30)
    #3 0x7fe9f52bd6a8 in sxqk_imgb_rebirth (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x7c6a8)
    #4 0x7fe9f52ae7f8 in maet_picbuf_alloc2 (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x6d7f8)
    #5 0x7fe9f52928c0 in maetd_dec (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x518c0)
    #6 0x7fe9f5293ce0 in maetd_decode (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52ce0)
    #7 0x7fe9f5290390 in _Z16read_maetel_argbPKN4SPen6StringEPiS3_S3_ (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x4f390)
    #8 0x7fe9facaa058 in _Z11ProcessFilePc (/home/test/notesfuzz/spiloader/spiloader+0x3058)
    #9 0x7fe9facaa190 in main (/home/test/notesfuzz/spiloader/spiloader+0x3190)
    #10 0x7fe9ed56e0f4 in __libc_init (/home/test/samsung/system/lib64/libc.so+0xca0f4)
```

heap-use-after-free___libqasan_free_libqasan.so+0x47e0.spi

```
==16139==ERROR: QEMU-AddressSanitizer: heap-use-after-free on address 0x7f60d426ff5f at pc 0x7f6157e9b758 bp 0x7f615ece3b70 sp
0x7f615ece3b10
READ of size 8 at 0x7f60d426ff5f thread T16139
    #0 0x7f6157e9b758 in __libqasan_free /home/test/qasan/qasan/libqasan/malloc.c:187
    #1 0x7f6157e99d40 in free /home/test/qasan/qasan/libqasan/hooks.c:169
    #2 0x7f6157891524 in maetd_pull_frm (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51524)
    #3 0x7f615789159c in maetd_pull_frm (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x5159c)
    #4 0x7f6157891f7c in maetd_flush (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x51f7c)
    #5 0x7f6157892a48 in maetd_delete (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x52a48)
    #6 0x7f615788f5dc in _Z16read_maetel_argbPKN4SPen6StringEPiS3_S3_ (/tmp/newnote/lib/arm64-v8a/libSPenBase.so+0x4f5dc)
    #7 0x7f6162fc7058 in _Z11ProcessFilePc (/home/test/notesfuzz/spiloader/spiloader+0x3058)
    #8 0x7f6162fc7190 in main (/home/test/notesfuzz/spiloader/spiloader+0x3190)
    #9 0x7f615758f0f4 in __libc_init (/home/test/samsung/system/lib64/libc.so+0xca0f4)
    #10 0x7f6162fc61e0 in __atexit_handler_wrapper (/home/test/notesfuzz/spiloader/spiloader+0x21e0)
```

heap-use-after-free_maet_set_ipm_libSPenBase.so+0x6a73c.spi
heap-use-after-free_maetd_eco_intra_nat_libSPenBase.so+0x59d10.spi
heap-use-after-free_maetd_eco_skip_ext_libSPenBase.so+0x58ee4.spi
heap-use-after-free_syscall_libc.so+0x1f330.spi