author	Gaosheng Cui <cuigaosheng1@huawei.com>	2022-10-31 19:25:36 +0800
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2022-11-25 17:40:16 +0100
commit	dbaab08c8677d598244d21afb7818e44e1c5d826 (patch)	
tree	bd58e43fedc937f486d776954ad7b355dcde8bb2	
parent	a597f8f710b3ecdbf1ad4430ec287febdd42d9c5 (diff)	
download	linux-dbaab08c8677d598244d21afb7818e44e1c5d826.tar.gz	

diff options

context: 3

space: include

mode: unified

capabilities: fix undefined behavior in bit shift for CAP_TO_MASK

```
[ Upstream commit 46653972e3ea64f79e7f8ae3aa41a4d3fdb70a13 ]

Shifting signed 32-bit value by 31 bits is undefined, so changing
significant bit to unsigned. The UBSAN warning calltrace like below:

UBSAN: shift-out-of-bounds in security/commoncap.c:1252:2
left shift of 1 by 31 places cannot be represented in type 'int'
Call Trace:
 <TASK>
 dump_stack_lvl+0x7d/0xa5
 dump_stack+0x15/0x1b
 ubsan_epilogue+0xe/0x4e
 __ubsan_handle_shift_out_of_bounds+0x1e7/0x20c
 cap_task_prctl+0x561/0x6f0
 security_task_prctl+0x5a/0xb0
 __x64_sys_prctl+0x61/0x8f0
 do_syscall_64+0x58/0x80
 entry_SYSCALL_64_after_hwframe+0x63/0xcd
 </TASK>

Fixes: e338d263a76a ("Add 64-bit capability support to the kernel")
Signed-off-by: Gaosheng Cui <cuigaosheng1@huawei.com>
Acked-by: Andrew G. Morgan <morgan@kernel.org>
Reviewed-by: Serge Hallyn <serge@hallyn.com>
Signed-off-by: Paul Moore <paul@paul-moore.com>
Signed-off-by: Sasha Levin <sashal@kernel.org>
```

Diffstat

-rw-r--r-- include/uapi/linux/capability.h 2

1 files changed, 1 insertions, 1 deletions

```
diff --git a/include/uapi/linux/capability.h b/include/uapi/linux/capability.h
index 240fdb9a60f685..6e0d68e841cdbc 100644
--- a/include/uapi/linux/capability.h
+++ b/include/uapi/linux/capability.h
@@ -376,7 +376,7 @@ struct vfs_ns_cap_data {
   */

 #define CAP_TO_INDEX(x)     ((x) >> 5)        /* 1 << 5 == bits in __u32 */
-#define CAP_TO_MASK(x)      (1 << ((x) & 31)) /* mask for indexed __u32 */
+#define CAP_TO_MASK(x)      (1U << ((x) & 31)) /* mask for indexed __u32 */
```

```
#endif /* _UAPI_LINUX_CAPABILITY_H */
```