author	Borys Popławski <borysp@invisiblethingslab.com>	2022-10-05 00:59:03 +0200
committer	Borislav Petkov <bp@suse.de>	2022-11-08 20:34:05 +0100
commit	f0861f49bd946ff94fce4f82509c45e167f63690 (patch)	
tree	fba0ba0ad4864609e5520a8322c634ac0b423435	
parent	f0c4d9fc9cc9462659728d168387191387e903cc (diff)	
download	linux-f0861f49bd946ff94fce4f82509c45e167f63690.tar.gz	

x86/sgx: Add overflow check in sgx_validate_offset_length()

```
sgx_validate_offset_length() function verifies "offset" and "length"
arguments provided by userspace, but was missing an overflow check on
their addition. Add it.

Fixes: c6d26d370767 ("x86/sgx: Add SGX_IOC_ENCLAVE_ADD_PAGES")
Signed-off-by: Borys Popławski <borysp@invisiblethingslab.com>
Signed-off-by: Borislav Petkov <bp@suse.de>
Reviewed-by: Jarkko Sakkinen <jarkko@kernel.org>
Cc: stable@vger.kernel.org # v5.11+
Link: https://lore.kernel.org/r/0d91ac79-6d84-abed-5821-4dbe59fa1a38@invisiblethingslab.com
```

Diffstat

-rw-r--r-- arch/x86/kernel/cpu/sgx/ioctl.c 3

1 files changed, 3 insertions, 0 deletions

```
diff --git a/arch/x86/kernel/cpu/sgx/ioctl.c b/arch/x86/kernel/cpu/sgx/ioctl.c
index ebe79d60619f2f..da8b8ea6b063d6 100644
--- a/arch/x86/kernel/cpu/sgx/ioctl.c
+++ b/arch/x86/kernel/cpu/sgx/ioctl.c
@@ -356,6 +356,9 @@ static int sgx_validate_offset_length(struct sgx_encl *encl,
        if (!length || !IS_ALIGNED(length, PAGE_SIZE))
                return -EINVAL;

+       if (offset + length < offset)
+               return -EINVAL;
+
        if (offset + length - PAGE_SIZE >= encl->size)
                return -EINVAL;
```