



index : kernel/git/stable/linux.git

master



switch

Linux kernel stable tree

Stable Group

[about](#) [summary](#) [refs](#) [log](#) [tree](#) [commit](#) [diff](#) [stats](#)

log msg



search

author Borys Popławski <borysp@invisiblethingslab.com> 2022-10-05 00:59:03 +0200
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-12-02 17:41:00 +0100
commit [5277e3d633a5d4157987f4aff068caa55e36db19](#) (patch)
tree [7292fe1bd199410ad8730fad5f8016d2f260dc64](#)
parent [b5a838ba47f285aa123eb08c0c790b1345c41859](#) (diff)
download [linux-5277e3d633a5d4157987f4aff068caa55e36db19.tar.gz](#)

diff options

context:

3



space:

include



mode:

unified



x86/sgx: Add overflow check in sgx_validate_offset_length()

[Upstream commit [f0861f49bd946ff94fce4f82509c45e167f63690](#)]

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-abad-5821-4dbe59fa1a38@invisiblethingslab.com>

Signed-off-by: Sasha Levin <sasha@kernel.org>

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 a66795e0b685a2..217777c029eea6 100644

--- a/arch/x86/kernel/cpu/sgx/ioctl.c

+++ b/arch/x86/kernel/cpu/sgx/ioctl.c

@@ -386,6 +386,9 @@ 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;