🏠 / Security / Security Advisories / Advisory TFMV-8

Advisory TFMV-8

Title	**Unchecked user-supplied pointer via mailbox messages may cause write of arbitrary address.**
CVE ID	CVE-2024-45746
Public Disclosure Date	October 02, 2024
Versions Affected	All version from TF-Mv1.6.0 up to TF-Mv2.1.0 inclusive
Configurations	Platforms with standard mailbox dispatcher `tfm_spe_mailbox`.
Impact	The mailbox message could contain arbitrary pointers which, in case of psa_call failure, would lead to write to a user-specified adddress in memory.
Fix Version	5ae0a02e8 TF-M v2.1.1
Credit	Infineon Technologies AG, in collaboration with: Tobias Scharnowski, Simon Wörner and Johannes Willbold from fuzzware.io.

Background

The psa_call message through the mailbox contains input/output vectors along with their respective lengths. This message is provided by a NSPE client. SPE takes the message and pass it to the mailbox dispatcher (tfm_spe_mailbox), which handles the message by performing a copy of the i/o vectors into local arrays. When either the client_id translation or the psa_call fails, the dispatcher replies immediately to the client. At that moment, the outvec is written back for its given length, which may not have been sanitized beforehand, resulting in arbitrary access of memory if the provided length goes beyond the legit vector size.

Impact

When the dispatcher in tfm_spe_mailbox is used, a user through mailbox could write into arbitrary address by first placing the malicious data into the local vectors with a bad message, then subsequently sending a psa_call with an invalid vector length. If both calls fail, the reply routine in tfm_spe_mailbox could take the injected data and write it into a desired location specified by the invalid length. Note that the above sequence would require sending the two mesages through two different mailbox slots.

Mitigation

Ensure that the outvec is written back only when the psa operation is successful. Any errors ahead of replying must be taken as a hint to avoid such write-back since they may be due to wrong supplied user-data in the vectors (pointers, length etc). To achieve the above, proper sanitization of input data must also be performed and related errors propagated to the reply subroutine.