Advisory TFMV-7

Title	ARoT can access PRoT data via debug logging functionality
CVE ID	CVE-2023-51712
Public Disclosure Date	The issue was publicly reported on 2023.12.04
Versions Affected	All version up to TF-M v2.0.0 inclusive
Configurations	IPC mode with TFM_SP_LOG_RAW_ENABLED=1
Impact	A malicious ARoT partition can expose any part of memory via stdio interface if TFM_SP_LOG_RAW_ENABLED is set
Fix Version	TBD
Credit	Roman Mazurak, Infineon

Background

TF-M log subsystem if enabled by `TFM_SP_LOG_RAW_ENABLED` config option, uses a supervisor call to print logging messages on the stdio output interface. Since the supervisor handler has the highest privilege level and full memory access, this communication channel can be exploited to expose any memory content to stdout device, usually UART. The logging subsystem is available to the secure side only but in isolation level 2 and higher PSA Root of Trust partitions (PRoT) shall be protected from an access from Application Root of Trust (ARoT) partitions. Although a direct call of `tfm_hal_output_sp_log()` from ARoT partition will be blocked by MPU raising the `MemoryManagement()` exception, a malicious ARoT partition can create an alternative call to the Supervisor to output any memory data like this:

```
static int tfm_output_unpriv_string(const unsigned char *str, size_t len)
{
    __ASM volatile("SVC %0         \n"
                   "BX LR          \n"
                    : : "I" (2));
}
```

Impact

In IPC mode with PSA isolation level 2 and higher and `TFM_SP_LOG_RAW_ENABLED` option enabled an ARoT partition can expose to the stdout device any memory data using TF-M logging subsystem via a call to the Supervisor.

Mitigation

Ensure that data sent for logging belong to the current partition. For that purpose `tfm_hal_memory_check(curr_partition->boundary, data, size, TFM_HAL_ACCESS_READABLE)` is added to the logging function of the Supervisor handler. If the check fails then data is ignored and `PSA_ERROR_NOT_PERMITTED` returns.
