Advisory TFMV-9

Title	FWU does not check the length of the TLV's payload
CVE ID	CVE-2025-53022
Public Disclosure Date	Jul 21, 2025
Versions Affected	All version from TF-M v1.3.0 up to TF-M v2.2.0 inclusive
Configurations	Any with Firmware Update (FWU) partition enabled
Impact	A Type-Length-Value (TLV) payload can be larger than the image dependency resulting in out-of-bounds write
Fix Version	c0e9727891dd395fbe274cfb052d8be741ea2942
Credit	Bartek Piekarski Distinguished Engineer, Product Security, Arm Ltd.

Background

In Firmware Update partition, the `fwu_bootloader_install_image()` function checks the authenticity and integrity of the image candidates. For each image candidate, its dependencies are loaded and when criteria are met, the candidate image is staged. During the dependencies check, the length of the image dependency fetched from the TLV is not verified, and this could lead to overflow in read and write from memory in subsequent steps.

Impact

An incorrect and unchecked TLV data can result in accessing the reading and writing memory for the candidate images that goes beyond the bounds, possibly causing in a redirection of program execution.

Mitigation

Add a length check in the `fwu_bootloader_install_image()` immediately after the next TLV is found by `bootutil_tlv_iter_next()`, during the dependencies fetch. See commit c0e9727891dd395fbe274cfb052d8be741ea2942.
