# CWE Detail – CWE-1193

## Description

The product enables components that contain untrusted firmware before memory and fabric access controls have been enabled.

## Extended Description

After initial reset, System-on-Chip (SoC) fabric access controls and other
 security features need to be programmed by trusted firmware as part
 of the boot sequence. If untrusted IPs or peripheral microcontrollers
 are enabled first, then the untrusted component can master
 transactions on the hardware bus and target memory or other assets to
 compromise the SoC boot firmware.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-1
* CAPEC-180

## Attack TTPs

**•** T1574.010: Services File Permissions Weakness (Tactics: persistence, privilege-escalation, defense-evasion)

## Common Consequences

**•** Impact: Bypass Protection Mechanism — Notes: An untrusted component can master transactions on the HW bus and target memory or other assets to compromise the SoC boot firmware.

## Potential Mitigations

**•** Architecture and Design: The boot sequence should enable fabric access controls and memory protections before enabling third-party hardware IPs and peripheral microcontrollers that use untrusted firmware. (Effectiveness: N/A)