# CWE Detail – CWE-1190

## Description

The product enables a Direct Memory Access (DMA) capable device before the security configuration settings are established, which allows an attacker to extract data from or gain privileges on the product.

## Extended Description

DMA is included in a number of devices because it allows
 data transfer between the computer and the connected device, using
 direct hardware access to read or write directly to main memory
 without any OS interaction. An attacker could exploit this to
 access secrets. Several virtualization-based mitigations have been introduced to thwart DMA attacks. These are usually
 configured/setup during boot time. However, certain IPs that are
 powered up before boot is complete (known as early boot IPs) may
 be DMA capable. Such IPs, if not trusted, could launch DMA
 attacks and gain access to assets that should otherwise be
 protected.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-180

## Attack TTPs

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

## Modes of Introduction

**•** Architecture and Design: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism, Modify Memory — Notes: DMA devices have direct write access to main memory and
 due to time of attack will be able to bypass OS or Bootloader
 access control.

## Potential Mitigations

**•** Architecture and Design: Utilize an IOMMU to orchestrate IO access from
 the start of the boot process. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)