# CWE Detail – CWE-1273

## Description

The credentials necessary for unlocking a device are shared across multiple parties and may expose sensitive information.

## Extended Description

"Unlocking a device" often means activating certain unadvertised debug and manufacturer-specific capabilities of a device using sensitive credentials. Unlocking a device might be necessary for the purpose of troubleshooting device problems. For example, suppose a device contains the ability to dump the content of the full system memory by disabling the memory-protection mechanisms. Since this is a highly security-sensitive capability, this capability is "locked" in the production part. Unless the device gets unlocked by supplying the proper credentials, the debug capabilities are not available. For cases where the chip designer, chip manufacturer (fabricator), and manufacturing and assembly testers are all employed by the same company, the risk of compromise of the credentials is greatly reduced. However, the risk is greater when the chip designer is employed by one company, the chip manufacturer is employed by another company (a foundry), and the assemblers and testers are employed by yet a third company. Since these different companies will need to perform various tests on the device to verify correct device function, they all need to share the unlock key. Unfortunately, the level of secrecy and policy might be quite different at each company, greatly increasing the risk of sensitive credentials being compromised.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Related Attack Patterns (CAPEC)

* CAPEC-560

## Attack TTPs

**•** T1078: Valid Accounts (Tactics: defense-evasion, persistence, privilege-escalation, initial-access)

## Modes of Introduction

**•** Integration: N/A

**•** Manufacturing: N/A

## Common Consequences

**•** Impact: Modify Memory, Read Memory, Modify Files or Directories, Read Files or Directories, Modify Application Data, Execute Unauthorized Code or Commands, Gain Privileges or Assume Identity, Bypass Protection Mechanism — Notes: Once unlock credentials are compromised, an attacker can use the credentials to unlock the device and gain unauthorized access to the hidden functionalities protected by those credentials.

## Potential Mitigations

**•** Integration: Ensure the unlock credentials are shared with the minimum number of parties and with utmost secrecy. To limit the risk associated with compromised credentials, where possible, the credentials should be part-specific. (Effectiveness: N/A)

**•** Manufacturing: Ensure the unlock credentials are shared with the minimum number of parties and with utmost secrecy. To limit the risk associated with compromised credentials, where possible, the credentials should be part-specific. (Effectiveness: N/A)

## Applicable Platforms

**•** VHDL (Class: None, Prevalence: Undetermined)

**•** Verilog (Class: None, Prevalence: Undetermined)

**•** None (Class: Compiled, Prevalence: Undetermined)

## Demonstrative Examples

**•** When the credentials of multiple organizations are stored together, exposure to third parties occurs frequently.

## Notes

**•** Maintenance: This entry is still under development and will continue to see updates and content improvements.