# CWE Detail – CWE-1254

## Description

The product's comparison logic is performed over a series of steps rather than across the entire string in one operation. If there is a comparison logic failure on one of these steps, the operation may be vulnerable to a timing attack that can result in the interception of the process for nefarious purposes.

## Extended Description

Comparison logic is used to compare a variety of objects including passwords, Message   
 Authentication Codes (MACs), and responses to verification challenges. When comparison logic is   
 implemented at a finer granularity (e.g., byte-by-byte comparison) and breaks in the case of a   
 comparison failure, an attacker can exploit this implementation to identify when exactly   
 the failure occurred. With multiple attempts, the attacker may be able to guesses the correct   
 password/response to challenge and elevate their privileges.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2019-10482: Smartphone OS uses comparison functions that are not in constant time, allowing side channels

**•** CVE-2019-10071: Java-oriented framework compares HMAC signatures using String.equals() instead of a constant-time algorithm, causing timing discrepancies

**•** CVE-2014-0984: Password-checking function in router terminates validation of a password entry when it encounters the first incorrect character, which allows remote attackers to obtain passwords via a brute-force attack that relies on timing differences in responses to incorrect password guesses, aka a timing side-channel attack.

## Related Attack Patterns (CAPEC)

* CAPEC-26

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Implementation: The hardware designer should ensure that comparison logic is implemented so as to compare in one operation instead in smaller chunks. (Effectiveness: N/A)

## Applicable Platforms

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

## Notes

**•** Maintenance: CWE 4.16 removed a demonstrative example for a hardware module because it was inaccurate and unable to be adapted. The CWE team is developing an alternative.