# CWE Detail – CWE-345

## Description

The product does not sufficiently verify the origin or authenticity of data, in a way that causes it to accept invalid data.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2022-30260: Distributed Control System (DCS) does not sign firmware images and only relies on insecure checksums for integrity checks

**•** CVE-2022-30267: Distributed Control System (DCS) does not sign firmware images and only relies on insecure checksums for integrity checks

**•** CVE-2022-30272: Remote Terminal Unit (RTU) does not use signatures for firmware images and relies on insecure checksums

## Related Attack Patterns (CAPEC)

* CAPEC-111
* CAPEC-141
* CAPEC-142
* CAPEC-148
* CAPEC-218
* CAPEC-384
* CAPEC-385
* CAPEC-386
* CAPEC-387
* CAPEC-388
* CAPEC-665
* CAPEC-701

## Attack TTPs

**•** T1491: Defacement (Tactics: impact)

**•** T1542.002: Component Firmware (Tactics: persistence, defense-evasion)

**•** T1584.002: DNS Server (Tactics: resource-development)

**•** T1557.002: ARP Cache Poisoning (Tactics: credential-access, collection)

**•** T1556: Modify Authentication Process (Tactics: credential-access, defense-evasion, persistence)

**•** T1211: Exploitation for Defense Evasion (Tactics: defense-evasion)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

**•** Impact: Varies by Context, Unexpected State — Notes:

## Applicable Platforms

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

## Demonstrative Examples

**•** Multiple vendors did not sign firmware images.

## Notes

**•** Relationship: "origin validation" could fall under this.

**•** Maintenance: The specific ways in which the origin is not properly identified should be laid out as separate weaknesses. In some sense, this is more like a category.