# CWE Detail – CWE-1357

## Description

The product is built from multiple separate components, but it uses a component that is not sufficiently trusted to meet expectations for security, reliability, updateability, and maintainability.

## Extended Description

Many modern hardware and software products are built by combining multiple smaller components together into one larger entity, often during the design or architecture phase. For example, a hardware component might be built by a separate supplier, or the product might use an open-source software library from a third party. Regardless of the source, each component should be sufficiently trusted to ensure correct, secure operation of the product. If a component is not trustworthy, it can produce significant risks for the overall product, such as vulnerabilities that cannot be patched fast enough (if at all); hidden functionality such as malware; inability to update or replace the component if needed for security purposes; hardware components built from parts that do not meet specifications in ways that can lead to weaknesses; etc. Note that a component might not be trustworthy even if it is owned by the product vendor, such as a software component whose source code is lost and was built by developers who left the company, or a component that was developed by a separate company that was acquired and brought into the product's own company. Note that there can be disagreement as to whether a component is sufficiently trustworthy, since trust is ultimately subjective. Different stakeholders (e.g., customers, vendors, governments) have various threat models and ways to assess trust, and design/architecture choices might make tradeoffs between security, reliability, safety, privacy, cost, and other characteristics.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2020-9054: Chain: network-attached storage (NAS) device has a critical OS command injection (CWE-78) vulnerability that is actively exploited to place IoT devices into a botnet, but some products are "end-of-support" and cannot be patched (CWE-1277). [REF-1097] (KEV)

## Modes of Introduction

**•** Requirements: Requirements might include criteria for which the only available solutions are provided by insufficiently trusted components.

**•** Architecture and Design: An insufficiently trusted component might be selected because it is less expensive to do in-house, requires expertise that is not available in-house, or might allow the product to reach the market faster.

## Common Consequences

**•** Impact: Reduce Maintainability — Notes:

## Potential Mitigations

**•** Requirements: For each component, ensure that its supply chain is well-controlled with sub-tier suppliers using best practices. For third-party software components such as libraries, ensure that they are developed and actively maintained by reputable vendors. (Effectiveness: N/A)

**•** Architecture and Design: Maintain a Bill of Materials for all components and sub-components of the product. For software, maintain a Software Bill of Materials (SBOM). According to [REF-1247], "An SBOM is a formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships." (Effectiveness: N/A)

**•** Operation: Continue to monitor changes in each of the product's components, especially when the changes indicate new vulnerabilities, end-of-life (EOL) plans, supplier practices that affect trustworthiness, etc. (Effectiveness: N/A)

## Notes

**•** Maintenance: As of CWE 4.10, the name and description for this entry has undergone significant change and is still under public discussion, especially by members of the HW SIG.