snyk snyk.io

# Snyk CWE Top 10 KEV (2023) Report

Report Executed by **hwajung7.lee@lge.com**

Report Executed on **2025-06-08**

Report Executed for **TestPresso**

Analysis Includes: **Snyk Code**

Additional Scope Filters:

| | |
|---|---|
| **Project Name** | hwajung7lee/SEC2_TripleS_RUI(main) |
| | hwajung7lee/SEC2_TripleS_dump1090(master) |

## Report Contents

## Section 1: Report Status

CWE Top 10 KEV Weaknesses: **Pass**

Analysis Includes: **Snyk Code**

# Section 2: About CWE Top 10 KEV

From https://cwe.mitre.org/top25/archive/2023/2023_kev_insights.html:

> In 2021, the Cybersecurity and Infrastructure Security Agency (CISA) began publishing the “Known Exploited Vulnerabilities (KEV) Catalog.” Entries in this catalog are vulnerabilities that have been reported through the Common Vulnerabilities and Exposures (CVE®) program and are observed to be (or have been) actively exploited. CISA recommends that organizations monitor the KEV catalog and use its content to help prioritize remediation activities in their systems to reduce the likelihood of compromise.
>
> By examining the CWE root cause mappings of vulnerabilities known to have been exploited in the wild, we gain new insight into what weaknesses adversaries exploit (as opposed to those most often reported by developers and researchers). 289 CVE Records were analyzed, comprising all the 2021 and 2022 CVE Records in the KEV catalog. Together with the 2023 CWE Top 25, the first ever Top 10 KEV Weaknesses List (using the same scoring methodology used for the 2023 Top 25) provides further information that organizations can use in their efforts to mitigate risk.

## Top 10 Known Exploited Vulnerabilities (KEV) Weaknesses list for 2023:

- **CWE-416: Use After Free** The program continues to use an object after it has been freed, leading to undefined behavior.
- **CWE-122: Heap-based Buffer Overflow** A heap overflow condition is a buffer overflow, where the buffer that can be overwritten is allocated in the heap portion of memory.
- **CWE-787: Out-of-bounds Write** The product writes data past the end, or before the beginning, of the intended buffer.
- **CWE-20: Improper Input Validation** The product does not validate or incorrectly validates user-controllable input before it is used as an input to a sensitive function.
- **CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')** The product constructs an OS command with external input and uses it in an unsafe way.
- **CWE-502: Deserialization of Untrusted Data** The product deserializes data that can be modified by an attacker, allowing the attacker to control the state or the flow of execution.
- **CWE-918: Server-Side Request Forgery (SSRF)** The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.
- **CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')**The product allocates or initializes a resource such as a pointer, object, or variable using one type, but it later accesses that resource using a type that is incompatible with the original type.
- **CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')** The product uses external input to construct a pathname that should be within a restricted directory, but it does not properly neutralize sequences such as ".." that can resolve to a location that is outside of that directory.
- **CWE-306: Missing Authentication for Critical Function** The software does not require authentication for a functionality that requires a provable user identity or consumes a significant amount of resources, allowing unauthorized access to this functionality.

# Section 3: Snyk’s Adherence to CWE Top 10 KEV

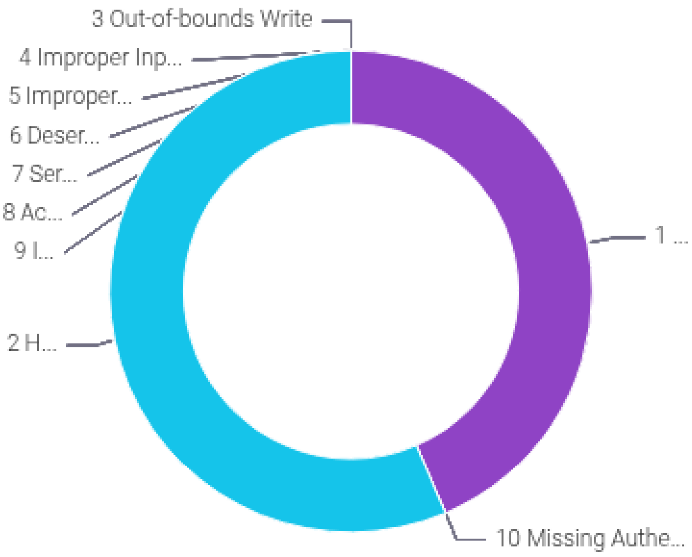
Snyk’s products detect issues in customer applications. Customers who want to align with the CWE Top 10 KEV list for managing their security issues can leverage this report to determine their compliance.

Snyk will produce a "**Pass**" status if no critical or high-severity issues map to the CWE Top 10 KEV list at the time of the report generation according to the scope selected. Snyk will produce a “**Did not pass**” status if critical or high-severity issues exist.

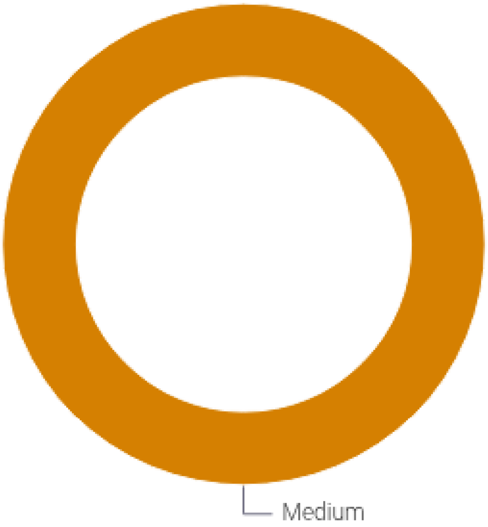
The report will reference any medium or low-severity issues found in Section 4: Issue Summary, but these issues will not result in a status of “Did not pass.” Medium or low severity issues can be found in the Snyk app and will not be included in Section 5: Issue Detail section.

# Section 4: Issue Summary

## Distribution of controls



## Issues by Severity



## Control details

| Control | CWE | C Critical | H High | M Medium | L Low | Total |
|---|---|---|---|---|---|---|
| ● 1 Use After Free | CWE-416 | 0 | 0 | 17 | 0 | 17 |
| ● 2 Heap-based Buffer Overflow | CWE-122 | 0 | 0 | 22 | 0 | 22 |
| ● 3 Out-of-bounds Write | CWE-787 | 0 | 0 | 0 | 0 | 0 |
| ● 4 Improper Input Validation | CWE-20 | 0 | 0 | 0 | 0 | 0 |
| ● 5 Improper Neutralization of Special Elements used in an OS Command (OS Command Injection) | CWE-78 | 0 | 0 | 0 | 0 | 0 |
| ● 6 Deserialization of Untrusted Data | CWE-502 | 0 | 0 | 0 | 0 | 0 |
| ● 7 Server-Side Request Forgery (SSRF) | CWE-918 | 0 | 0 | 0 | 0 | 0 |

| Control | CWE | C Critical | H High | M Medium | L Low | Total |
|---|---|---|---|---|---|---|
| ● 8 Access of Resource Using Incompatible Type (Type Confusion) | CWE-843 | 0 | 0 | 0 | 0 | 0 |
| ● 9 Improper Limitation of a Pathname to a Restricted Directory (Path Traversal) | CWE-22 | 0 | 0 | 0 | 0 | 0 |
| ● 10 Missing Authentication for Critical Function | CWE-306 | 0 | 0 | 0 | 0 | 0 |
| All Controls | | 0 | 0 | 39 | 0 | 39 |

## Section 5: Issue Detail

Empty custom HTML visualization

## Section 6: Snyk Methodology

### What is Snyk?

Snyk is a developer security platform that enables application and cloud developers to secure their whole application — finding and fixing vulnerabilities from their first lines of code to their running cloud.

### Industry-leading security intelligence

Snyk security researchers augment their expertise with advanced ML and human-in-the-loop AI so we can provide the most accurate, timely and comprehensive intelligence on the market. This security intel is the foundation of our platform, spanning the Snyk Vulnerability Database, the Snyk Code knowledge base, and our Cloud/IaC unified policy engine.

### Snyk Severity Levels

A severity level is applied to a vulnerability, to indicate the risk for that vulnerability in an application.

Severity levels are key factors in vulnerability assessment, and can be:

| Severity | Severity Level | Description |
|---|---|---|
| C | Critical | This may allow attackers to access sensitive data and run code on your application |
| H | High | This may allow attackers to access sensitive data in your application |
| M | Medium | Under some conditions, this may allow attackers to access sensitive data on your application |
| L | Low | Application may expose some data that allows vulnerability mapping, which can be used with other vulnerabilities to attack the application |

### Determining severity levels - Snyk Open Source and Snyk Container

The Common Vulnerability Scoring System (CVSS) determines the severity level of a vulnerability.

Snyk uses CVSS framework version 3.1 to communicate the characteristics and severity of vulnerabilities.

| Severity | Severity Level | CVSS score |
|---|---|---|
| L | Low | 0.0 - 3.9 |
| M | Medium | 4.0 - 6.9 |
| H | High | 7.0 - 8.9 |
| C | Critical | 9.0 - 10.0 |

The severity level and score are determined based on the CVSS Base Score calculations using the Base Metrics.

See Scoring security vulnerabilities 101: Introducing CVSS for CVEs to learn more.

Severity levels may not always align with CVSS scores. For example, Snyk Container severity scores for Linux vulnerabilities may vary depending on NVD severity rankings; see Understanding Linux vulnerability severity for more details.

For more information about CVSS and severity levels please see the following documentation.