Snyk Top 10: Go OSS Vulnerabilities 2022

These are the most prevalent **critical and high** open source vulnerabilities found by Snyk scans of Go apps in 2022.

01 Denial of Service (DoS)

Denial of service (DoS) describes a family of attacks, all aimed at making a system inaccessible to its intended and legitimate users. Attackers will attempt to trigger system crashes or spike resources to make services inoperable.

Top vuln: CVE-2022-28948
Fix: Upgrade `github.com/go-yaml/yaml to version 3.0.0` or higher.

02 NULL Pointer Dereference

A null pointer dereference is a specific type of null dereference that occurs when you try to access an object reference that has a null value in a programming language that uses pointers.

Top vuln: CVE-2020-29652
Fix: Upgrade `Amazon-Linux:2 golang to version 0:1.18.3-1.amzn2` or higher.

03 Out-of-Bounds Read

The application reads data outside of the intended buffer, either from the beginning or end. This can allow attackers to access information they don't have proper permissions to or cause a crash that could lead to a denial of service.

Top vuln: CVE-2021-38561
Fix: Upgrade `golang.org/x/text/internal/language` to version 0.3.7 or higher.

04 Authorization Bypass

This is when an attacker gains access to a system or data without proper authorization. They are able to obtain the privileges of an authorized user without having to authenticate.

Top vuln: Unassigned CWE-285
Fix: Upgrade `github.com/emicklei/go-restful` to version 2.16.0 or higher.

05 Authorization Bypass Through User-Controlled Key

An error in a system's authorization functionality that allows an attacker to gain access to user data. This can be done by when a user-controlled key has not been properly validated or when a key has been intentionally or accidentally leaked.

Top vuln: CVE-2022-1996
Fix: There is no fixed version for `Debian:unstable golang-github-emicklei-go-restful`.

06 Buffer Overflow

A type of runtime error that allows a program to write past the end of a buffer or array and corrupt adjacent memory. This can cause the buffer to overflow, which can corrupt other parts of the program or allow an attacker to gain access to the system.

Top vuln: CVE-2021-43784
Fix: Upgrade `github.com/opencontainers/runc/libcontainer` to version 1.0.3 or higher.

07 Out-of-Bounds

The application reads or writes data outside of the intended memory buffer. This can allow attackers to access information they don't have proper permissions to or cause a crash that could lead to a denial of service.

Top vuln: CVE-2022-44797
Fix: Upgrade `github.com/btcsuite/btcd/wire` to version 0.23.2 or higher.

08 Symlink Attack

This occurs when a package is vulnerable to an attackers' request for a seemingly innocuous container configuration that results in the host filesystem being bind-mounted into the container.

Top vuln: CVE-2021-30465
Fix: Upgrade `github.com/opencontainers/runc/libcontainer` to version 1.0.0-rc95 or higher.

09 Improper Output Neutralization for Logs

This vulnerability — also known as log forging — occurs when attackers are able to either forge lines in a log file or inject malicious content into a log.

Top vuln: CVE-2020-36567
Fix: There is no fixed version for `Debian:10 golang-github-gin-gonic-gin`.

10 Improper Preservation of Permissions

This vulnerability occurs if permissions are either not preserved or preserved incorrectly when copy, sharing, or restoring objects. This can lead to unintentionally granting access to objects that had previously been restricted.

Top vuln: CVE-2021-43816
Fix: Upgrade `github.com/containerd/containerd/pkg/cri` to version 1.5.9 or higher.