# **Snyk Top 10:** .NET OSS Vulnerabilities 2022

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

## 01 Insecure Defaults

Insecure default vulnerabilities occur when a product initializes with a value or values that aren't the aren't secure. They can occur when products are designed so administrators are expected to change the defaults before making an application available (ex: admin/admin).

**Top vuln:** Unassigned CWE-755
**Fix:** Upgrade `Newtonsoft.Json` to version 13.0.1 or higher.

## 02 Remote Code Execution (RCE)

Remote code execution (RCE) allows an attacker to execute arbitrary code on a remote device. This is often done through injection attacks. In 2022, a big RCE vulnerability was Spring4Shell.

**Top vuln:** CVE-2021-26701
**Fix:** Upgrade `System.Text.Encodings.Web` to version 4.5.1, 4.7.2, 5.0.1 or higher.

## 03 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-2022-29117
**Fix**: Upgrade `Centos:8 dotnet` to version 0:6.0.105-1.el8_6 or higher.

## 04 Directory Traversal

A directory traversal attack aims to access files and directories that are stored outside the intended folder. By manipulating files with "dot-dot-slash (../)" sequences and their variations, or by using absolute file paths, it may be possible to access arbitrary files and directories stored on the filesystem.

**Top vuln**: CVE-2021-32840
**Fix**: Upgrade `SharpZipLib` to version 1.3.3 or higher.

## 05 Regular Expression Denial of Service (ReDoS)

The regular expression denial of service (ReDoS) is a type of denial of service attack. Regular expressions are incredibly powerful, but they aren't very intuitive and can ultimately end up making it easy for attackers to take your site down.

**Top vuln:** CVE-2021-21252
**Fix:** Upgrade jQuery.Validation to version 1.19.3 or higher.

## 06 Privilege Escalation

Privilege escalation is when a user or system obtains more permissions to a resource than they were allowed. These permissions are obtained by exploiting a weakness in the system. Keep in mind the principle of least privilege.

**Top vuln**: CVE-2022-41032
**Fix:** Upgrade `Alpine:3.16 dotnet6-build` to version 6.0.110-r0 or higher.

## 07 Arbitrary Code Execution (ACE)

Arbitrary code execution (ACE) happens when an attacker is able to run commands or execute code of their choice on a target machine. If this code is executed over a network, it is sometimes referred to as remote code execution.

**Top vuln**: CVE-2021-46703
**Fix:** There is no fixed version for `RazorEngine.`

## 08 Improper Verification of Cryptographic Signature

Improper verification of cryptographic signatures occurs when an application fails to properly verify the authenticity of a digital signature. This may allow attackers to alter or forge signatures without detection and will create security vulnerabilities, such as allowing attackers to impersonate legitimate users or modify signed messages without detection.

**Top vuln:** CVE-2021-43569
**Fix**: Upgrade `starkbank-ecdsa` to version 1.3.2 or higher.

## 09 Use After Free

This occurs when an application continues to use memory after it has been freed or deallocated. This can create a security vulnerability by allowing attackers to manipulate or control the freed memory.

**Top vuln**: CVE-2022-0609
**Fix**: Upgrade `CefSharp.Common` to version 98.1.210 or higher.

## 10 Cross-Site Scripting (XSS)

Cross-site scripting is a website attack method that utilizes a type of injection to implant malicious scripts into websites that would otherwise be productive and trusted. Generally, the process consists of sending a malicious browser-side script to another user.

**Top vuln:** CVE-2020-26293
**Fix:** Upgrade `HtmlSanitizer` to version 5.0.372 or higher.

**Find and automatically fix OSS vulns in your .NET apps for free with Snyk.**

Start free