

Snyk Top 10: C# Vulnerabilities 2022



These are the most prevalent C# vulnerabilities found by Snyk Code researchers in 2022.

01

Cross-Site Request Forgery (CSRF)

Cross-site request forgery (CSRF) is a vulnerability where an attacker performs actions while impersonating another user. For example, transferring funds to an attacker's account, changing a victim's email address, or even redirecting a pizza to an attacker's address!

[Learn more about this vulnerability](#)

04

Use of Hardcoded Credentials

Hardcoded credentials are used for inbound authentication, outbound communication to external components, and encryption of internal data. However, they can create holes that allow attackers to bypass the system authentication, which are often difficult to detect and fix.

[Learn more about this vulnerability](#)

07

Improper Use of Validation Framework

Improper use of validation occurs when the product incorrectly implements, or fails to use, an input validation framework from the source language or an independent library. This can lead to future exploitable conditions if input validation isn't completed later in the development cycle.

[Learn more about this vulnerability](#)

09

Cryptographic Issues

This class of cryptographic vulnerabilities is related to the design and implementation of data confidentiality and integrity. The weaknesses in this category could lead to a degradation in data quality if they aren't addressed.

[Learn more about this vulnerability](#)

02

Directory Traversal

A directory traversal (a.k.a. path traversal) attack aims to access files and directories that are stored outside the intended folder. Manipulating files with "dot-dot-slash (../)" sequences, or absolute file paths, can provide access to arbitrary files and directories stored on the file system.

[Learn how to mitigate at Snyk Learn](#)

05

ASP.NET Misconfiguration: Creating Debug Binary

This misconfiguration vulnerability occurs when an ASP.NET application has been configured to produce debug binaries in a production environment. These binaries give detailed debugging messages and create security risks when used outside of development or testing environments

[Learn more about this vulnerability](#)

08

Open Redirect

An open redirect vulnerability occurs when an application allows a user to control a redirect or forward to another URL. If untrusted user input isn't validated, an attacker could supply a URL that redirects an unsuspecting victim from a legitimate domain to an attacker's phishing site.

[Learn how to mitigate at Snyk Learn](#)

10

Deserialization

Deserialization is a mechanism to convert byte streams into application data. Insecure deserialization is a vulnerability that occurs when attacker-controlled data is deserialized by the server. In the worst case, it can lead to remote code execution.

[Learn more about this vulnerability](#)

03

Insecure Hash

An insecure hash vulnerability is a failure related to cryptography, which is the way we encrypt or hash data. By having an insecure hash there is a high chance that your confidential data will be exposed.

[Learn how to mitigate at Snyk Learn](#)

06


Log Forging

Log forging is a vulnerability that occurs when data enters an application from an untrusted source, or is written into an application or system log file. A successful log forging attack could lead to other injection-style attacks like XSS and PHP parsing.

[Learn more about this vulnerability](#)

Find and automatically fix vulns in your C# apps for free with Snyk.

[Start free](#)



snyk TOP 10