Snyk Top 10: Ruby OSS Vulnerabilities 2022

snyk

These are the most prevalent **critical and high** open source vulnerabilities found by Snyk scans of Ruby 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-2022-30122
Fix: Upgrade `rack` to version 2.0.9.1, 2.2.3.1 or higher.

02 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-2022-24836

Fix: Upgrade `nokogiri` to version 1.13.4 or higher.

03 Arbitrary Code Injection

A type of attack that allows malicious users to inject malicious code into an application through a user input field, which is then executed on the fly.

Top vuln: CVE-2022-30123
Fix: Upgrade `rack` to version 2.0.9.1, 2.1.4.1, 2.2.3.1 or higher.

04 NULL Pointer Deference

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: Unassigned CWE-476
Fix: Upgrade `nokogiri` to version 1.13.9-aarch64-linux or higher.

05 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, the big RCE vulnerability was Spring4Shell.

Top vuln: CVE-2022-32224
Fix: Upgrade `activerecord` to version 5.2.8.1, 6.0.5.1, 6.1.6.1, 7.0.3.1 or higher.

06 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-2022-31163
Fix: Upgrade `tzinfo` 0.3.61, 1.2.10 or higher.

07 Out-of-Bounds Write

This vulnerability occurs when data is written outside of the expected buffer — either before or after — creating unexpected behaviors on later writes. These behaviors can include crashes, corruption, and execution.

Top vuln: CVE-2018-25032
Fix: Upgrade nokogiri to version 1.13.4 or higher.

08 Improper Handling of Unexpected Data Type

Any code that receives input should validate the input to verify that is the expected data type, otherwise unexpected behaviors can occur. For example, if an application expects an integer, but gets a string, improper handling could result in a crash as it attempts to perform arithmetic operations on characters.

Top vuln: CVE-2022-29181
Fix: Upgrade `nokogiri` to version 1.13.6-aarch64-linux 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-2022-23308
Fix: Upgrade nokogiri to version 1.13.2 or higher.

10 Information Exposure

This is a type of broken access control vulnerability in which a user or attacker gains access to information that they are not explicitly authorized to view, including PII, company data, system data/metadata, and more.

Top vuln: CVE-2022-23633
Fix: Upgrade `actionpack` to version 5.2.6.2, 6.0.4.6, 6.1.4.6, 7.0.2.2 or higher.