Snyk Top 10: Python OSS Vulnerabilities 2022

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

01 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-2022-40899
Fix: Upgrade `future` to version 0.18.3 or higher.

02 SQL Injection

SQL injection is a common method used by attackers to manipulate and access database information. This is done by exploiting application vulnerabilities to inject malicious SQL code that alters SQL queries.

Top vuln: CVE-2022-34265
Fix: Upgrade `Debian:12 python-django` to version 2:4.0.6-1 or higher.

03 Denial of Service

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-2021-20270
Fix: Upgrade `Pygments` to version 2.7.4 or higher.

04 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-2022-21699
Fix: Upgrade `ipython` to version 7.16.3, 7.31.1, 8.0.1 or higher.

05 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-2022-3786
Fix: Upgrade `cryptography` to version 38.0.3 or higher.

06 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-2022-24439
Fix: Upgrade `GitPython` to version 3.1.30 or higher.

07 Reflected File Download

In an RFD attack, the attacker creates a malicious file and the user opens it without verifying the origin. This can allow an attacker to execute unsafe code.

Top vuln: CVE-2022-36359
Fix: Upgrade `django` to version 3.2.15, 4.0.7, 4.1 or higher.

08 Command Injection

Command injection attacks — also known as operating system command injection attacks — exploit a programming flaw to execute system commands without proper input validation, escaping, or sanitization, which may lead to arbitrary commands executed by a malicious attacker.

Top vuln: CVE-2022-45907
Fix: Upgrade `torch` to version 1.13.1 or higher.

09 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-2022-41902
Fix: Upgrade `tensorflow` to version 2.8.4, 2.9.3, 2.10.1 or higher.

10 Improper Privilege Management

Improper privilege management occurs when an application or system fails to properly control and manage user privileges. If an application or system does not properly manage user privileges, it can allow users to perform actions that they are not authorized to perform.

Top vuln: CVE-2022-39286
Fix: Upgrade `jupyter-core` to version 4.11.2 or higher.