Snyk Top 10: JavaScript OSS Vulnerabilities 2022

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

01 Prototype Pollution

Prototype pollution is an injection attack that targets JavaScript runtimes. An attacker might control the default values of an object's properties. This allows the attacker to tamper with the logic of the application.

Top vuln: CVE-2021-43138
Fix: Upgrade `async` to version 2.6.4, 3.2.2, 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-2021-3807
Fix: Upgrade `Debian:10` `node-ansi-regex` to version 3.0.0-1+deb10u1 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-2022-38900
Fix: Upgrade `decode-uri-component` to version 0.2.2 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-2022-24785
Fix: Upgrade `moment` to version 2.29.2 or higher.

05 Improper Input Validation

Improper input validation is when the application receives input (or data) but it does not take the necessary steps to validate the input or it simply incorrectly validates the input. This can lead to your application receiving unintended input which may result in altered data or arbitrary code execution.

Top vuln: CVE-2022-2421
Fix: Upgrade `socket.io-parser` to version 3.3.3, 3.4.2, 4.0.5, 4.2.1 or higher.

06 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-2022-25898
Fix: Upgrade `jsrsasign` to version 10.5.25 or higher.

07 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-2022-29078
Fix: Upgrade `ejs` to version 3.1.7 or higher.

08 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-2016-20018
Fix: Upgrade `knex` to version 2.4.0 or higher.

09 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-2022-0355
Fix: Upgrade `simple-get` to version 2.8.2, 3.1.1, 4.0.1 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-2022-0144
Fix: Upgrade `shelljs` to version 0.8.5 or higher.