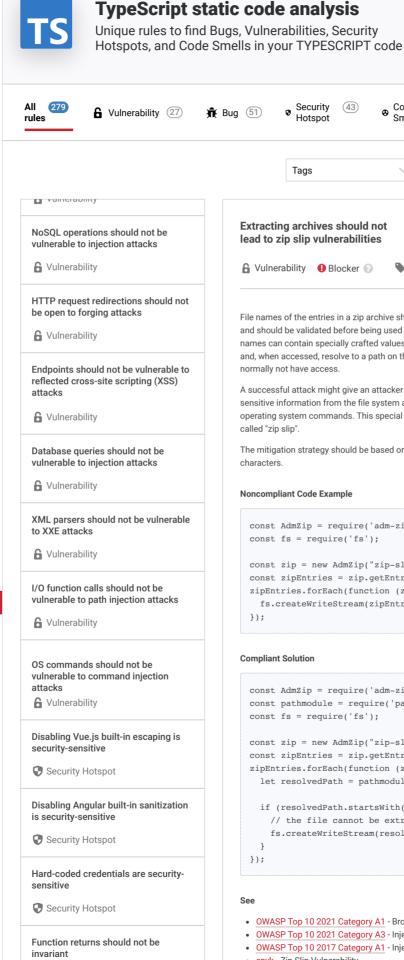


Products ✓





```
⊗ Code
                                                              O Quick 50 Fix
                    Security
                              (43)
                                                 (158)
# Bug (51)
                   Hotspot
                                          Smell
                                                 Search by name.
                   Tags
       Extracting archives should not
                                                       Analyze your code
       lead to zip slip vulnerabilities
        injection cwe owasp sans-top25
       File names of the entries in a zip archive should be considered untrusted, tainted
       and should be validated before being used for file system operations. Indeed, file
       names can contain specially crafted values, such as '../', that change the initial path
       and, when accessed, resolve to a path on the filesystem where the user should
       normally not have access.
       A successful attack might give an attacker the ability to read, modify, or delete
       sensitive information from the file system and sometimes even execute arbitrary
       operating system commands. This special case of path injection vulnerabilities is
       called "zip slip"
       The mitigation strategy should be based on the whitelisting of allowed paths or
       characters.
       Noncompliant Code Example
         const AdmZip = require('adm-zip');
         const fs = require('fs');
         const zip = new AdmZip("zip-slip.zip");
         const zipEntries = zip.getEntries();
         zipEntries.forEach(function (zipEntry) {
            fs.createWriteStream(zipEntry.entryName); // Noncompliant
         });
       Compliant Solution
         const AdmZip = require('adm-zip');
         const pathmodule = require('path');
         const fs = require('fs');
         const zip = new AdmZip("zip-slip.zip");
         const zipEntries = zip.getEntries();
```

});

OWASP Top 10 2021 Category A1 - Broken Access Control

zipEntries.forEach(function (zipEntry) {

let resolvedPath = pathmodule.join(__dirname + '/archive_t

if (resolvedPath.startsWith(__dirname + '/archive_tmp')) {

// the file cannot be extracted outside of the "archive_ fs.createWriteStream(resolvedPath); // Compliant

- OWASP Top 10 2021 Category A3 Injection
- OWASP Top 10 2017 Category A1 Injection
- snyk Zip Slip Vulnerability
- MITRE, CWE-20 Improper Input Validation

Code Smell

Assertions should be complete
Code Smell

Tests should include assertions
Code Smell

Octal values should not be used
Code Smell

Switch cases should end with an unconditional "break" statement
Code Smell

"switch" statements should not

MITRE, CWE-22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
 MITRE, CWE-99 - Improper Control of Resource Identifiers ('Resource Injection')
 MITRE, CWE-641 - Improper Restriction of Names for Files and Other Resources
 SANS Top 25 - Risky Resource Management

Available In:
Sonarcloud Sonarqube
Developer Edition

© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved.

Privacy Policy