NVD DB Update

CVE-2025-24964 - Score: 9.6

Components:

Description:

Vitest is a testing framework powered by Vite. Affected versions are subject to arbitrary remote Code Execution when accessing a malicious website while Vitest API server is listening by Cross-site WebSocket hijacking (CSWSH) attacks. When ‘api‘ option is enabled (Vitest UI enables it), Vitest starts a WebSocket server. This WebSocket server did not check Origin header and did not have any authorization mechanism and was vulnerable to CSWSH attacks. This WebSocket server has ‘saveTestFile‘ API that can edit a test file and ‘rerun‘ API that can rerun the tests. An attacker can execute arbitrary code by injecting a code in a test file by the ‘saveTestFile‘ API and then running that file by calling the ‘rerun‘ API. This vulnerability can result in remote code execution for users that are using Vitest serve API. This issue has been patched in versions 1.6.1, 2.1.9 and 3.0.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.

Main problems:

1385 no CWE Description available