NVD DB Update

CVE-2024-12450 - Score: 9.8

Components:

infiniflow ragflow 0.12.0

Description:

In infiniflow/ragflow versions 0.12.0, the ‘web_crawl‘ function in ‘document_app.py‘ contains multiple vulnerabilities. The function does not filter URL parameters, allowing attackers to exploit Full Read SSRF by accessing internal network addresses and viewing their content through the generated PDF files. Additionally, the lack of restrictions on the file protocol enables Arbitrary File Read, allowing attackers to read server files. Furthermore, the use of an outdated Chromium headless version with --no-sandbox mode enabled makes the application susceptible to Remote Code Execution (RCE) via known Chromium v8 vulnerabilities. These issues are resolved in version 0.14.0.

Main problems:

77 no CWE Description available