MEDIUM

Search by package name or CVE

Content Injection

Affecting Crow package, versions [,0.3+4)

INTRODUCED: 12 JAN 2022 CVE-2021-23824 CWE-79

Share

How to fix?

Upgrade `Crow` to version 0.3+4 or higher.

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><img src={{src}} /></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 PR
- GitHub Release

Snyk CVSS

Attack Complexity	Low

See more

NVD 6.1 MEDIUM

Snyk ID	SNYK-UNMANAGED-CROW-2336164
Published	12 Jan 2022
Disclosed	12 Jan 2022
Credit	Snyk Security Team

Report a new vulnerability Found a mistake?

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon

Join the >>
community