4 CVE-2022-27779: cookie for trailing dot TLD

Share:

TIMELINE

haxatron1 submitted a report to curl. Apr 28th (7 months ago)

Summary:

In CVE-2014-3620 curl prevents cookies from being set for Top Level Domains (TLDs). According to the advisory, curl's "cookie parser has no Public Suffix awareness", but it will "reject TLDs from being allowed". However, a cookie can still be set for a TLD + trailing dot.

A trailing dot after a TLD is considered legal and curl will send the http://example.com. to http://example.com

Steps To Reproduce:

1. Create an Apache file like the following

Code 46 Bytes Wrap lines Copy Download

```
1  <?php
2
3  header("Set-Cookie: a=b; Domain=.me.");
```

2. Now save the cookie to curl and see the cookie is set for .me.

Code 50 Bytes Wrap lines Copy Download

```
1  curl -c cookies.txt http://localtest.me./index.php
```

cookies.txt:

Code 180 Bytes Wrap lines Copy Download

```
1  # Netscape HTTP Cookie File
2  # https://curl.se/docs/http-cookies.html
3  # This file was generated by libcurl! Edit at your own risk.
```

3. Requests sent via curl to the domain with TLD + "." will now contain the particular cookie.

Code 47 Bytes — Wrap lines Copy Download

```
curl -b cookies.txt http://domain.me./index.php
```

Code 79 Bytes — Wrap lines Copy Download

```
GET / HTTP/1.1
Host: domain.me.
User-Agent: curl/7.83.0
Accept: */*
Cookie: a=b
```

Impact

Cookies can be set by arbitrary sites for TLD + ".", and if a trailing dot is used for an unrelated site, curl will send the cookie to the unrelated site.

bagder curl staff posted a comment. Apr 28th (7 months ago)

Thank you for your report!

We will take some time and investigate your reports and get back to you with details and possible follow-up questions as soon as we can!

bagder curl staff posted a comment. Apr 28th (7 months ago)

Confirmed.

curl supports PSL since 2015, if you build curl with libspsl it will not accept this cookie. If you really want secure cookie handling, going without PSL seems like bad a idea. If you build curl without PSL support it will accept cookies for numerous domains which opens it up for leaking cookies between unrelated sites and it cannot do anything about that.

curl should however still reject cookies set for nothing but a TLD. Here, I believe we can attribute this to our friend "trailing dots in host names". The gift that just keeps offering pain in different ways.

In commit b27ad8e1d3e68e (shipped in 7.83.0) we recently modified the trailing-dot handling and as a result it seems we broke this cookie domain treatment for non-PSL builds.

Attach here is test 977 which reproduces this problem when built without PSL, but correctly rejects the cookie when built *with* PSL...

bagder curl staff posted a comment. Apr 28th (7 months ago)

Probably fixed something like this:

Code 665 Bytes Wrap lines Copy Download

```
diff --git a/lib/cookie.c b/lib/cookie.c
index 451881f57..0c2d49b47 100644
--- a/lib/cookie.c
+++ b/lib/cookie.c
@@ -425,11 +425,19 @@ static void remove_expired(struct CookieInfo *cookies)
 }

 /* Make sure domain contains a dot or is localhost. */
 static bool bad_domain(const char *domain)
 {
-  return !strchr(domain, '.') && !strcasecompare(domain, "localhost");
+  if(strcasecompare(domain, "localhost"))
+    return FALSE;
+  else {
+    /* there must be a dot present, but that dot must not be a trailing dot */
+    char *dot = strchr(domain, '.');
+    if(dot)
+      return dot[1] ? FALSE : TRUE;
+  }
+  return TRUE;
 }

 /*
  * Curl_cookie_add
  *

```

haxatron1 posted a comment. Apr 28th (7 months ago)

I can confirm that the above patch fixes the issue.

dgustafsson curl staff posted a comment. Apr 28th (7 months ago)

Patch LGTM.

bagder curl staff posted a comment. Apr 29th (7 months ago)

@haxatron1 how would you like to be credited in the security advisory and on the curl site etc?

This is what I have right now:

```
This issue was reported by Haxatron on hackerone. Patched by Daniel Stenberg.
```

bagder curl staff updated CVE reference to CVE-2022-27779. Apr 29th (7 months ago)

Apr 29th (7 months ago)

bagder curl staff changed the report title from **Bypass CVE-2014-3620 via trailing dot after TLD** to **CVE-2022-27779: cookie for trailing dot TLD**.

haxatron1 posted a comment. Apr 29th (7 months ago)

Hi, you can use my name: Axel Chong

Thanks!

bagder curl staff posted a comment. Apr 29th (7 months ago)

Advisory draft.

1 attachment:
F1711667: CVE-2022-27779.md

haxatron1 posted a comment. Apr 29th (7 months ago)

Details look good to me! But my name is Axel, not Alex.

bagder curl staff posted a comment. Apr 29th (7 months ago)

Oops. Sorry about that. I've corrected my local version now.

bagder curl staff posted a comment. Apr 29th (7 months ago)

The plan is right now to do a patch release (7.83.1) on May 11 with this flaw patched and announce this vulnerability in sync with that.

bagder curl staff posted a comment. Apr 30th (7 months ago)

I double-checked and it does not reproduce with 7.81.0

bagder curl staff posted a comment. May 5th (7 months ago)

I have notified distros@openwall about this issue now. Set for announcement with the pending release on May 11.

bagder curl staff closed the report and changed the status to ○ **Resolved**. May 11th (7 months ago)

Published. This issue is now eligible for a bounty claim from IBB.

bagder curl staff requested to disclose this report. May 11th (7 months ago)

haxatron1 posted a comment. May 11th (7 months ago)

Hi I think range 27778-27780 html files is missing on the curl project website

https://curl.se/docs/CVE-2022-27778.html
https://curl.se/docs/CVE-2022-27779.html
https://curl.se/docs/CVE-2022-27780.html

bagder curl staff posted a comment. May 11th (7 months ago)

They just need a few more minutes, they should be there just about... now

haxatron1 agreed to disclose this report. May 11th (7 months ago)

This report has been disclosed. May 11th (7 months ago)

curl has decided that this report is not eligible for a bounty. May 13th (7 months ago)

Thanks for your work. The actual monetary reward part for this issue is managed by the Internet Bug Bounty so the curl project itself therefor sets the reward amount to **zero USD**. If you haven't already, please submit your reward request to them and refer back to this issue.