Bug 5106 - Broken cache manager URL parsing

Status: RESOLVED FIXED

Alias: None

Product: Squid
Component: other (show other bugs)
Version: unspecified
Hardware: All All

Importance: P5 blocker
Assignee: SQUID BUGS ALIAS

URL:

Depends on:
Blocks:

Reported: 2021-03-03 17:02 UTC by Joshua Rogers
Modified: 2021-05-07 09:55 UTC (History)
CC List: 0 users

See Also:
Browser: ---
Fixed Versions: 4.15, 5.0.6

Attachments

Add an attachment (proposed patch, testcase, etc.)

Note
You need to log in before you can comment on or make changes to this bug.

Joshua Rogers 2021-03-03 17:02:25 UTC Description

Hi there,

There is an easy-to-reproduce exception which is luckily caught triggered from cache_manager.cc:

If the page 'cache_object://0/io?&' is accessed, CacheManager::ParseUrl() will parse the URL as follows:

```
t = sscanf(url, "cache_object://%[^/]/%[^?]%n?%s", host, request, &pos, params);
```

This 'params' variable will then be passed: Mgr::QueryParams::Parse(params, cmd->params.queryParams).

At this stage, 'params' contains only a single character, '&'.

As the function goes on, it is picked up here:

```
for (size_t i = n; i < len; ++i) {
if (aParamsStr[i] == '&') {
if (!ParseParam(aParamsStr.substr(n, i), param))
```

here, both 'n' and 'i' are 0.

aParamsStr.substr(n, i) thus causes an exception:

```
Breakpoint 8, String::substr (this=0x7fffffff3860, from=0, to=0) at String.cc:226
226         Must(from < size());
(gdb) n
227         Must(to > 0 && to <= size());
(gdb) n
2021/03/03 16:58:58.743| 0,3| String.cc(227) substr: check failed: to > 0 && to <=
size()
    exception location: String.cc(227) substr
2021/03/03 16:58:58.761| 33,3| ../../src/base/AsyncJobCalls.h(178) dial:
Server::doClientRead threw exception: check failed: to > 0 && to <= size()
    exception location: String.cc(227) substr
2021/03/03 16:58:58.761| 93,2| AsyncJob.cc(129) callException: check failed: to > 0
&& to <= size()
    exception location: String.cc(227) substr
```

A one-line reproducer:

```
printf "GET cache_object://0/io?&\n" | nc localhost 3128
```

Alex Rousskov 2021-03-03 20:02:53 UTC Comment 1

I can reproduce in v4-based code.

Amos Jeffries 2021-03-14 00:39:51 UTC Comment 2

FTR, there is no longer any need for this logic to be parsing the full URI. There is a pre-parsed and validated representation available at HttpRequest::url which shoudl be the argument passed to this function. At most the Uri::path string may need parsing to identify the command and params segments.

Amos Jeffries 2021-03-14 01:27:45 UTC Comment 3

Since AnyP::Uri is my project I will pick this up and make a PR shortly.

Amos Jeffries 2021-03-16 02:48:15 UTC Comment 4

https://github.com/squid-cache/squid/pull/788

Amos Jeffries 2021-05-07 09:55:21 UTC Comment 5

.
