Bug 1244505 - Firefox 44 no longer allows spaces in cookie names, breaking some apps

Last Comment

Status: VERIFIED FIXED
Whiteboard:
Keywords: compat, dev-doc-complete, regression, site-compat, testcase

Product: Core (show info)
Component: Networking: Cookies (show other bugs) (show info)
Version: Trunk
Platform: Unspecified Unspecified

Importance: -- normal (vote)
Target Milestone: mozilla47
Assigned To: Nicholas Hurley [:nwgh][:hurley]
QA Contact:
Mentors:

URL:

Duplicates: ~~1243783~~ (view as bug list)
Depends on:
Blocks: ~~1233784~~
Show dependency tree / graph

Reported: 2016-01-30 21:12 PST by Kohei Yoshino [:kohei]
Modified: 2016-02-08 17:31 PST (History)
CC List: 17 users (show)

Flags: andrei.vaida: qe-verify+
See Also:

Crash Signature: (edit)
QA Whiteboard:
Iteration: ---
Points: ---
Has Regression Range: ---
Has STR: ---
Project Flags:
Tracking Flags:

tracking-firefox44:	+
status-firefox44:	verified
tracking-firefox45:	+
status-firefox45:	verified
tracking-firefox46:	+
status-firefox46:	verified
tracking-firefox47:	+
status-firefox47:	verified
relnote-firefox:	44+

Attachments

Allow spaces in cookie names (1.43 KB, patch) 2016-02-01 09:47 PST, Nicholas Hurley [:nwgh][:hurley]	mcmanus: review+ sledru: approval-mozilla-aurora+ sledru: approval-mozilla-beta+ sledru: approval-mozilla-release+	Details | Diff | Review
test patch (1.61 KB, patch) 2016-02-04 10:15 PST, Nicholas Hurley [:nwgh][:hurley]	mcmanus: review+	Details | Diff | Review
testcase (254 bytes, text/html) 2016-02-04 10:37 PST, Kohei Yoshino [:kohei]	*no flags*	Details
Add an attachment (proposed patch, testcase, etc.)		View All

Kohei Yoshino [:kohei] 2016-01-30 21:12:42 PST — Description

I know whitespaces are now allowed in cookie names, guess the behaviour has been changed in ~~Bug 1233784~~. (I don't have access to the bug)

https://www.mozilla.org/en-US/security/advisories/mfsa2016-04/

But I have seen at least 2 reports regarding whitespaces in cookie names:

https://support.mozilla.org/en-US/questions/1107073
https://input.mozilla.org/en-US/dashboard/response/5795493

Is this change intended? If so, I'll write a site compatibility doc for Web developers.

Kohei Yoshino [:kohei] 2016-01-30 21:26:22 PST — Comment 1

I meant: whitespaces are *not* allowed in cookie names

Kohei Yoshino [:kohei] 2016-01-30 21:57:23 PST — Comment 2

Another report:
https://input.mozilla.org/en-US/dashboard/response/5795475

Perhaps related:
https://input.mozilla.org/en-US/dashboard/response/5792410
https://input.mozilla.org/en-US/dashboard/response/5793857

Kohei Yoshino [:kohei] 2016-01-30 23:57:03 PST — Comment 3

Posted the site compatibility doc: https://www.fxsitecompat.com/en-CA/docs/2016/whitespaces-are-no-longer-allowed-in-cookie-names/

Kohei Yoshino [:kohei] 2016-02-01 07:25:06 PST — Comment 4

There aren't so many reports from developers so far, but it's difficult to measure the impact of the change. For end users, they are just no longer able to sign into a site or use specific site features, and they don't know what should they do.

Should we allow spaces, not vertical tabs or whatever, for interoperability, maybe? My guess is all other browsers allow spaces for historical reasons, and that's why we are seeing reports from developers this time.

Kohei Yoshino [:kohei] 2016-02-01 07:44:09 PST — Comment 5

[Tracking Requested - why for this release]: A new site compatibility issue. Some apps are broken due to a side effect from a security fix in Firefox 44.

Nicholas Hurley [:nwgh][:hurley] 2016-02-01 09:29:08 PST — Comment 6

Let me dig up my notes from this - it may be worth backing out all or part of this change (this is the second bug I've seen today).

Nicholas Hurley [:nwgh][:hurley] 2016-02-01 09:38:12 PST — Comment 7

Quoting ~~https://bugzilla.mozilla.org/show_bug.cgi?id=1191423#c49~~ (since it's a security bug, and not generally open):

"I had a look at other browsers, and the status of compat there is much more consistent than with odd characters in the values. All browsers I tested (with the exception of Firefox) disallow any character 0x1e and below, as well as space (0x20). IE/Edge is the only browser other than Firefox that allows 0x1f in a name. Beyond that, it gets a bit messier, but not too crazy (safari is slightly stricter than everyone else). I think we're safe disallowing characters <= 0x20 to occur in the name."

Though now it's seeming that's not 100% true (maybe my test was faulty in some way). I propose changing the list of disallowed name characters (and *only* name characters) to *not* include 0x20 (space), as that seems the most likely culprit. Unfortunately, I won't be able to test the fix, as I don't have accounts on any of the affected sites.

Jason, Patrick, what do you think? (The patch is simple enough, will make it while I await response.)

Nicholas Hurley [:nwgh][:hurley] 2016-02-01 09:40:59 PST — Comment 8

*** ~~Bug 1243783~~ has been marked as a duplicate of this bug. ***

Nicholas Hurley [:nwgh][:hurley] 2016-02-01 09:47:33 PST — Comment 9

Created attachment 8714365 [details] [diff] [review]
Allow spaces in cookie names

Here's the patch to allow spaces in cookie names. Everything else that I originally disallowed still seems reasonable to disallow.

Patrick McManus [:mcmanus] 2016-02-02 09:04:37 PST — Comment 10

(In reply to Nicholas Hurley [:nwgh][:hurley] from comment #7)

> >
> Though now it's seeming that's not 100% true (maybe my test was faulty in

I think the only right answer here is maximum compat - let's do what chrome does. Can we figure out why your test doesn't match the reports?

Nicholas Hurley [:nwgh][:hurley] 2016-02-02 09:23:07 PST — Comment 11

Yeah, space is the only one I got wrong - my test did single-character names, not names containing certain characters (mixed with other, known-legal characters). When I changed, both safari and chrome accept 0x20 (safari also accepts 0x09 (\t), while chrome doesn't - we always disallowed \t). So, the patch I've put up seems like the right course.

Jason, no need from info from you, just an r+ would be good so we can get this fixed (or Patrick can feel free to steal the r+ if he wants).

Pulsebot 2016-02-02 11:13:21 PST — Comment 12

https://hg.mozilla.org/integration/mozilla-inbound/rev/2351a9ec305b

James 2016-02-03 01:13:37 PST — Comment 13

Could you confirm a timeframe for when the fix will be released / what version number

The internet has been broken for those users using firefox where sites have cookies with spaces and have had to use other browsers such as chrome / internet explorer

thanks

james

Carsten Book [:Tomcat] 2016-02-03 03:28:34 PST — Comment 14

https://hg.mozilla.org/mozilla-central/rev/2351a9ec305b

Patrick McManus [:mcmanus] 2016-02-03 08:16:28 PST — Comment 15

plz nom the backports

Nicholas Hurley [:nwgh][:hurley] 2016-02-03 08:39:03 PST — Comment 16

Comment on attachment 8714365 [details] [diff] [review]
Allow spaces in cookie names

Approval Request Comment
[Feature/regressing bug #]: 1233784
[User impact if declined]: Some sites unable to set cookies
[Describe test coverage new/current, TreeHerder]: On m-c, manual testing
[Risks and why]: Very low - this is a return to previous behavior, and matches Safari and Chrome
[String/UUID change made/needed]: None

chris hofmann 2016-02-03 17:52:01 PST — Comment 17

stack overflow article that lots of developers probably reference and appears at the top of google search results on related topics. the article traces the ugly and twisted history of cookie specification.

http://stackoverflow.com/questions/1969232/allowed-characters-in-cookies

might be worth pitching in a few comments on that thread if cross browser testing reviles different results than posted there.

probably would be good to have tests against the specs and defacto standards implemented in the other browsers to avoid the unlikely chance that changes happen again in this area in the future.

Doug Turner (:dougt) 2016-02-03 18:59:18 PST — Comment 18

Tests please?

chris hofmann 2016-02-03 20:55:47 PST — Comment 19

This article also has some interesting observations on the universe of cookie implementations

https://github.com/golang/go/issues/7243

Sylvestre Ledru [:sylvestre] 2016-02-04 03:53:59 PST — Comment 20

Comment on attachment 8714365 [details] [diff] [review]
Allow spaces in cookie names

Oh, this makes me sad...

Can I ask why we don't have tests for this? We should be checking for invalid cookies names and with all the codes in illegalNameCharacters
Until now, taking on the behalf of Ritu as she mentioned taking it in 44.0.1
Should be also in 45 beta 3.

James 2016-02-04 03:57:25 PST — Comment 21

We refer to the issue as cookiegate

Carsten Book [:Tomcat] 2016-02-04 05:43:49 PST — Comment 22

https://hg.mozilla.org/releases/mozilla-aurora/rev/9962682e5e75

Carsten Book [:Tomcat] 2016-02-04 06:08:28 PST — Comment 23

https://hg.mozilla.org/releases/mozilla-beta/rev/d6f5a4905c66

Carsten Book [:Tomcat] 2016-02-04 06:12:37 PST — Comment 24

https://hg.mozilla.org/releases/mozilla-release/rev/c51ca5032cf0

Kohei Yoshino [:kohei] 2016-02-04 09:39:42 PST — Comment 25

Updated the site compat doc: https://www.fxsitecompat.com/en-CA/docs/2016/whitespaces-are-no-longer-allowed-in-cookie-names/

Nicholas Hurley [:nwgh][:hurley] 2016-02-04 10:13:45 PST — Comment 26

(In reply to Sylvestre Ledru [:sylvestre] from comment #20)

> Can I ask why we don't have tests for this? We should be checking for
> invalid cookies names and with all the codes in illegalNameCharacters

There is a test, but it's not exhaustive; in other words, the test doesn't specifically test every single value in illegalNameCharacters - there's no point, as if it blocks one character in the array, it blocks them all (as we've seen in practice).

I will add a new test to ensure we continue allowing spaces in both names and values, though.

Nicholas Hurley [:nwgh][:hurley] 2016-02-04 10:15:37 PST — Comment 27

Created attachment 8715913 [details] [diff] [review]
test patch

Here's a test to ensure spaces stay allowed.

Ritu Kothari (:ritu) 2016-02-04 10:24:05 PST — Comment 28

Kohei, could you please verify that the fix works as expected on the latest Nightly build? Thanks!

Kohei Yoshino [:kohei] 2016-02-04 10:37:59 PST — Comment 29

Created attachment 8715924 [details]
testcase

Kohei Yoshino [:kohei] 2016-02-04 10:39:19 PST — Comment 30

LGTM on Nightly.

chris hofmann 2016-02-04 10:52:20 PST — Comment 31

yeah, the problem here is not that we needed an automated test to tell us if the characters we intended to block were actually blocked (although that kind of testing has some value).

The problem was in assessing how wide the use of the space character was in cookie names and values across the corpus of the web, or how ambitious we needed to be in blocking that specific character.

The best ways to figure that out would be to 1) find articles like the ones mentioned in comment 17 and 19 or 2) use things like bclary's web crawler to scan top sites *and* the dark corners of the web to determine actual use/depenency and frequency on the web.

The article in comment 19 represented a few months of kicking around how best to classify use of cookies on the web. It stated:

Comment 13:

Alternative proposal. Split bytes into three sets:

white: [0x21, 0x7e] minus double-quote, comma, semi-colon and backslash.
gray: 0x20 space and 0x2c comma.
black: everything else.

Drop any black bytes. If there are any gray bytes, quote the entire cookie value.
Otherwise (white bytes only), do not quote the value.

Under this classification we make some changes definitely in the "safe" blocking zone, but we made one change in the "grey" zone and that came back to bite us.

The one area of analysis that could still be done is to think about and understand how quoting works v. unquoted (double quoted) passing of characters, and how that works in all the browsers, and potentially on some websites. Its not clear if we have tested or thought about that much in bug comments, but maybe someone has.

one other lesson re-learned here. don't mess with lou montulli's cookie code without lots of time and effort and testing. ;-) That might be some of the oldest code remaining in the code base.

chris hofmann 2016-02-04 11:05:41 PST — Comment 32

> don't mess with lou montulli's cookie code without lots of time and effort and testing. ;-)

that should have been time and testing on the web, with analysis of user comments like appeared in this bug.

this also represented another case of a change that jumped trains and could have used longer bake time on nightly, beta, and aurora and time for random reports that said "this site doesn't work correctly for me anymore", and then investigations like what :kohei undertook.

GREAT JOB :kohei! Thanks for saving us before this change went to all users.

Petruta Rasa [QA] [:petruta] 2016-02-05 06:40:42 PST — Comment 33

Verified as fixed using the attached testcase with Firefox 44.0.1, Firefox 45 beta 3, latest Aurora 46.0a2 and latest Nightly 47.0a1 (2016-02-05) under Win 7 x64, Ubuntu 14.04 x64 and Mac OS X 10.9.5.

Kohei Yoshino [:kohei] 2016-02-05 10:41:44 PST — Comment 34

(In reply to chris hofmann from comment #32)

> GREAT JOB :kohei! Thanks for saving us before this change went to all users.

Yay. The finding is part of my Firefox Site Compatibility initiative :)
https://www.fxsitecompat.com/about/

Pulsebot 2016-02-05 13:49:04 PST — Comment 35

https://hg.mozilla.org/integration/mozilla-inbound/rev/140603de6df9

Phil Ringnalda (:philor) 2016-02-06 19:11:38 PST — Comment 36

https://hg.mozilla.org/mozilla-central/rev/140603de6df9

Sylvestre Ledru [:sylvestre] 2016-02-08 13:41:49 PST — Comment 37

Added in the release notes with "Allows spaces in cookie names (1244505)" as wording

Anthony 2016-02-08 15:21:09 PST — Comment 38

Have you considered that perhaps the applications that depend on SP in cookie names are themselves broken?

```
According to RFC 6265 HTTP State Management Mechanism, s4.1.1 Syntax:
cookie-name    = token
token          = <token, defined in [RFC2616], Section 2.2>

Consulting RFC 2616, s2.2 Basic Rules:
token          = 1*<any CHAR except CTLs or separators>
separators     = "(" | ")" | "<" | ">" | "@"
               | "," | ";" | ":" | "\" | <">
               | "/" | "[" | "]" | "?" | "="
               | "{" | "}" | SP | HT
```

So the requirement is that cookie names do not allow SP characters.

Nicholas Hurley [:nwgh][:hurley] 2016-02-08 16:50:29 PST — Comment 39

(In reply to Anthony from comment #38)

> Have you considered that perhaps the applications that depend on SP in
> cookie names are themselves broken?

Yes, according to RFC 6265, they are, in fact broken. That was why the change to disallow spaces was made in the first place. Unfortunately, however, the world we live in is not as cleanly defined as the RFC would hope - spaces are (as this bug indicates) rather common in the real world, and are allowed by other browsers. So, in the interest of operating on the internet we have (and not the internet we may wish we had), we'll continue allowing spaces in cookie names.

Anthony 2016-02-08 17:31:49 PST — Comment 40

(In reply to Nicholas Hurley [:nwgh][:hurley] from comment #39)

> So, in the interest of operating on the
> internet we have (and not the internet we may wish we had), we'll continue
> allowing spaces in cookie names.

This is disappointing and shows why the internet is such a broken place. Nobody is prepared to stick to the RFCs and Standards to improve interoperability. Instead we're reduced to the same level as that mother of the little misbehaving brat who keeps saying "aww, come on, let him do it" whenever he does something wrong.

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

Format For Printing - XML - Clone This Bug - Top of page