










Sign in


 [apache / httpd](#) Public


 Notifications


 Fork 1.1k


 Star 3.6k


 Code

 Pull requests 71

 Actions

 Projects

 Security

 Insights

Commit


core: AP_NORMALIZE_DECODE_UNRESERVED should normalize the second enco...


Browse files

...ded dot.


Otherwise ap_normalize_path() can leave some "%2e" encoded.

git-svn-id: <https://svn.apache.org/repos/asf/httpd/httpd/trunk@1893724> 13f79535-47bb-0310-9956-ffa450edef68

 Loading branch information

 ylavic committed on Sep 29, 2021

1 parent [cd70257](#) commit [e150697](#)

 Showing 2 changed files with 17 additions and 5 deletions.

Whitespace


Ignore whitespace



Split

Unified




Filter changed files

changes-entries

normalize_unreserved... 

2  changes-entries/normalize_unreserved.txt  ...

...	...	@@ -0,0 +1,2 @@
1	+	*) core: AP_NORMALIZE_DECODE_UNRESERVED should normalize the second dot in
2	+	the uri-path when it's preceded by a dot. [Yann Ylavic]

 20  server/util.c  ...

		@@ -503,7 +503,8 @@ static char x2c(const char *what);
503	503	AP_DECLARE(int) ap_normalize_path(char *path, unsigned int flags)
504	504	{

505	505	int ret = 1;
506	-	apr_size_t l = 1, w = 1;
	506	+ apr_size_t l = 1, w = 1, n;
	507	+ int decode_unreserved = (flags & AP_NORMALIZE_DECODE_UNRESERVED) != 0;
507	508	
508	509	if (!IS_SLASH(path[0])) {
509	510	/* Besides "OPTIONS *", a request-target should start with '/'
		@@ -530,7 +531,7 @@ AP_DECLARE(int) ap_normalize_path(char *path, unsigned int flags)
		* be decoded to their corresponding unreserved characters by
		* URI normalizers.
		*/
533	-	if ((flags & AP_NORMALIZE_DECODE_UNRESERVED)
	534	+ if (decode_unreserved
534	535	&& path[l] == '%' && apr_isxdigit(path[l + 1])
		&&
535	536	apr_isxdigit(path[l + 2])) {
536	537	const char c = x2c(&path[l + 1]);
		@@ -568,8 +569,17 @@ AP_DECLARE(int) ap_normalize_path(char *path, unsigned int flags)
		continue;
568	569	}
569	570	
570	571	
571	-	/* Remove /xx/.. segments */
572	-	if (path[l + 1] == '.' && IS_SLASH_OR_NUL(path[l + 2])) {
	572	+ /* Remove /xx/.. segments (or /xx/.%2e/ when
	573	+ * AP_NORMALIZE_DECODE_UNRESERVED is set since we
	574	+ * decoded only the first dot above).
	575	*/
	576	n = l + 1;
	577	if ((path[n] == '.' (decode_unreserved
	578	&& path[n]
		== '%'
	579	&&
		path[++n] == '2'

```
580 +                                &&
      (path[++n] == 'e'
581 +                                ||
      path[n] == 'E'))
582 +                                && IS_SLASH_OR_NUL(path[n +
      1])) {
573 583                                /* Wind w back to remove the
      previous segment */
574 584                                if (w > 1) {
575 585                                do {
@@ -586,7 +596,7 @@ AP_DECLARE(int)
ap_normalize_path(char *path, unsigned int flags)
586 596                                }
587 597
588 598                                /* Move l forward to the next
      segment */
589 -                                l += 2;
599 +                                l = n + 1;
590 600                                if (path[l]) {
591 601                                l++;
592 602                                }
.....
↓
```

0 comments on commit e150697

Please [sign in](#) to comment.

