muttmua / **mutt** Public

Code | Pull requests | Actions | Projects | Security and quality | Insights

Commit `12f54fe`

kevin8t8 committed 2 weeks ago

```
Check for embedded nul in url_pct_decode().

Consider %00 an invalid character in a URL.

Thanks to evilrabbit@tutamail.com for the security report.

Reviewed-by: Alejandro Colomar <alx@kernel.org>
```

`master` · mutt-2-3-2-rel

1 parent f547a84 commit 12f54fe

1 file changed +3 -1

Top

Filter files...

url.c

Search within code

url.c

```
@@ -60,7 +60,9 @@ static int url_pct_decode (char *s)
60  60          if (s[1] && s[2] &&
61  61          isxdigit ((unsigned char) s[1]) &&
62  62          isxdigit ((unsigned char) s[2]) &&
63      -       hexval (s[1]) >= 0 && hexval (s[2]) >= 0)
    63  +           hexval(s[1]) >= 0 && hexval(s[2]) >= 0 &&
    64  +           // check for embedded nul
    65  +           (hexval(s[1]) > 0 || hexval(s[2]) > 0))
64  66          {
65  67        *d++ = (hexval (s[1]) << 4) | (hexval (s[2]));
```

```
66    68          s += 2;
```

Comments 0