python / cpython Public

Code Issues 5k+ Pull requests 2.1k Actions Projects Security and q

Commit d16ecc6

3 people authored 3 weeks ago · 76 / 80 · Verified

```
[3.13] gh-145599, CVE 2026-3644: Reject control characters in
http.cookies.Morsel.update() (GH-145600) (#146024)

gh-145599, CVE 2026-3644: Reject control characters in `http.cookies.Morsel.update()` (GH-
145600)

Reject control characters in `http.cookies.Morsel.update()` and
`http.cookies.BaseCookie.js_output`.
(cherry picked from commit 57e88c1)

Co-authored-by: Stan Ulbrych <89152624+StanFromIreland@users.noreply.github.com>
Co-authored-by: Victor Stinner <vstinner@python.org>
Co-authored-by: Victor Stinner <victor.stinner@gmail.com>
```

3.13 (AcreetionOS-Linux/python#2, #146024) · v3.13.13

1 parent 196edfb commit d16ecc6

3 files changed +62 -4 lines changed

Top

Filter files…

- Lib
  - http
    - cookies.py
  - test
    - test_http_cookies.py
- Misc/NEWS.d/next/Security
  - 2026-03-06-17-03-38.gh-issue-145599.kchwZV.rst

3 files changed +62 -4 lines changed

Search within code

Lib/http/cookies.py

```
@@ -335,9 +335,16 @@ def update(self, values):
335 335                 key = key.lower()
336 336                 if key not in self._reserved:
337 337                     raise CookieError("Invalid attribute %r" % (key,))
338     +               if _has_control_character(key, val):
339     +                   raise CookieError("Control characters are not allowed in "
340     +                                     f"cookies {key!r} {val!r}")
338 341                 data[key] = val
339 342             dict.update(self, data)
340 343
344     +     def __ior__(self, values):
345     +         self.update(values)
346     +         return self
347     +
341 348         def isReservedKey(self, K):
342 349             return K.lower() in self._reserved
343 350
@@ -363,9 +370,15 @@ def __getstate__(self):
363 370             }
364 371
365 372         def __setstate__(self, state):
366     -           self._key = state['key']
367     -           self._value = state['value']
368     -           self._coded_value = state['coded_value']
373     +           key = state['key']
374     +           value = state['value']
375     +           coded_value = state['coded_value']
376     +           if _has_control_character(key, value, coded_value):
377     +               raise CookieError("Control characters are not allowed in cookies "
378     +                                 f"{key!r} {value!r} {coded_value!r}")
379     +           self._key = key
380     +           self._value = value
381     +           self._coded_value = coded_value
382
383         def output(self, attrs=None, header="Set-Cookie:"):
384             return "%s %s" % (header, self.OutputString(attrs))
@@ -377,13 +390,16 @@ def __repr__(self):
390
391         def js_output(self, attrs=None):
```

```
379  392            # Print javascript
     393  +         output_string = self.OutputString(attrs)
     394  +         if _has_control_character(output_string):
     395  +             raise CookieError("Control characters are not allowed in cookies")
380  396            return """
381  397            <script type="text/javascript">
382  398            <!-- begin hiding
383  399            document.cookie = \"%s\";
384  400            // end hiding -->
385  401            </script>
386       -         """ % (self.OutputString(attrs).replace('"', r'\"'))
     402  +         """ % (output_string.replace('"', r'\"'))
387  403
388  404        def OutputString(self, attrs=None):
389  405            # Build up our result
```

Lib/test/test_http_cookies.py

```
@@ -574,6 +574,14 @@ def test_control_characters(self):
574  574                with self.assertRaises(cookies.CookieError):
575  575                    morsel["path"] = c0
576  576
     577  +             # .__setstate__()
     578  +             with self.assertRaises(cookies.CookieError):
     579  +                 morsel.__setstate__({'key': c0, 'value': 'val', 'coded_value':
          'coded'})
     580  +             with self.assertRaises(cookies.CookieError):
     581  +                 morsel.__setstate__({'key': 'key', 'value': c0, 'coded_value':
          'coded'})
     582  +             with self.assertRaises(cookies.CookieError):
     583  +                 morsel.__setstate__({'key': 'key', 'value': 'val',
          'coded_value': c0})
     584  +
577  585              # .setdefault()
578  586              with self.assertRaises(cookies.CookieError):
579  587                  morsel.setdefault("path", c0)
@@ -588,6 +596,18 @@ def test_control_characters(self):
588  596              with self.assertRaises(cookies.CookieError):
589  597                  morsel.set("path", "val", c0)
590  598
```

```
599 +             # .update()
600 +             with self.assertRaises(cookies.CookieError):
601 +                 morsel.update({"path": c0})
602 +             with self.assertRaises(cookies.CookieError):
603 +                 morsel.update({c0: "val"})
604 +
605 +             # .__ior__()
606 +             with self.assertRaises(cookies.CookieError):
607 +                 morsel |= {"path": c0}
608 +             with self.assertRaises(cookies.CookieError):
609 +                 morsel |= {c0: "val"}
610 +
591 611         def test_control_characters_output(self):
592 612             # Tests that even if the internals of Morsel are modified
593 613             # that a call to .output() has control character safeguards.
    @@ -608,6 +628,24 @@ def test_control_characters_output(self):
608 628                 with self.assertRaises(cookies.CookieError):
609 629                     cookie.output()
610 630
631 +         # Tests that .js_output() also has control character safeguards.
632 +         for c0 in support.control_characters_c0():
633 +             morsel = cookies.Morsel()
634 +             morsel.set("key", "value", "coded-value")
635 +             morsel._key = c0  # Override private variable.
636 +             cookie = cookies.SimpleCookie()
637 +             cookie["cookie"] = morsel
638 +             with self.assertRaises(cookies.CookieError):
639 +                 cookie.js_output()
640 +
641 +             morsel = cookies.Morsel()
642 +             morsel.set("key", "value", "coded-value")
643 +             morsel._coded_value = c0  # Override private variable.
644 +             cookie = cookies.SimpleCookie()
645 +             cookie["cookie"] = morsel
646 +             with self.assertRaises(cookies.CookieError):
647 +                 cookie.js_output()
648 +
611 649
612 650     def load_tests(loader, tests, pattern):
613 651         tests.addTest(doctest.DocTestSuite(cookies))
```

...6-03-06-17-03-38.gh-issue-145599.kchwZV.rst

```
@@ -0,0 +1,4 @@
+ Reject control characters in :class:`http.cookies.Morsel`
+ :meth:`~http.cookies.Morsel.update` and
+ :meth:`~http.cookies.BaseCookie.js_output`.
+ This addresses :cve:`2026-3644`.
```

Comments 0