python / **cpython** Public

Code Issues 5k+ Pull requests 2.2k Actions Projects Security and q

⚠ This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.

Commit a2cdbb6

StanFromIreland authored on Oct 7, 2025 · ✕ 22 / 36 · Verified

```
[3.9] gh-121227: Disallow setting an empty list for NPN (GH-137161)
```

· v3.9.25 ••• 3.9

1 parent 312de66 commit a2cdbb6

3 files changed +10 -0 lines changed

Top

Filter files…

- Lib
  - ssl.py
  - test
    - test_ssl.py
- Misc/NEWS.d/next/Security
  - 2025-07-28-10-35-59.gh-issue-121227.Orp1wf.rst

3 files changed +10 -0 lines changed

Search within code

Lib/ssl.py

```
@@ -520,6 +520,8 @@ def wrap_bio(self, incoming, outgoing,
server_side=False,
520  520
521  521          def set_npn_protocols(self, npn_protocols):
```

```
522  522            protos = bytearray()
     523  +         if not npn_protocols:
     524  +             raise SSLError('NPN protocols must not be empty')
523  525            for protocol in npn_protocols:
524  526                b = bytes(protocol, 'ascii')
525  527                if len(b) == 0 or len(b) > 255:
```

Lib/test/test_ssl.py

```
@@ -4219,6 +4219,12 @@ def test_npn_protocols(self):
4219  4219                    if len(stats['server_npn_protocols']) else 'nothing'
4220  4220                self.assertEqual(server_result, expected, msg % (server_result,
      "server"))
4221  4221
     4222  +     def test_empty_npn_protocols(self):
     4223  +         """npn_protocols cannot be empty, see CVE-2024-5642 & gh-121227"""
     4224  +         client_context, server_context, hostname = testing_context()
     4225  +         with self.assertRaises(ssl.SSLError):
     4226  +             server_context.set_npn_protocols([])
     4227  +
4222  4228        def sni_contexts(self):
4223  4229            server_context = ssl.SSLContext(ssl.PROTOCOL_TLS_SERVER)
4224  4230            server_context.load_cert_chain(SIGNED_CERTFILE)
```

...5-07-28-10-35-59.gh-issue-121227.Orp1wf.rst

```
@@ -0,0 +1,2 @@
1  + Raise an :exc:`SSL.SSLError` if an empty *protocols* argument is passed to
2  + :meth:`ssl.SSLContext.set_npn_protocols` to fix ``CVE-2024-5642``.
```

Comments 0