NameVirtualHost Host header injection.

Low **adiroiban** published **GHSA-vg46-2rrj-3647** on Oct 26

Package

twisted (pip)

Affected versions	Patched versions
>=0.9.4	>=22.10.0rc1

Description

When the host header does not match a configured host `twisted.web.vhost.NameVirtualHost` will return a `NoResource` resource which renders the Host header unescaped into the 404 response allowing HTML and script injection.

In practice this should be very difficult to exploit as being able to modify the Host header of a normal HTTP request implies that one is already in a privileged position.

Example configuration:

```
from twisted.web.server import Site
from twisted.web.vhost import NameVirtualHost
from twisted.internet import reactor

resource = NameVirtualHost()
site = Site(resource)
reactor.listenTCP(8080, site)
reactor.run()
```

Output:

```
❯ curl -H"Host:<h1>HELLO THERE</h1>" http://localhost:8080/

<html>
  <head><title>404 - No Such Resource</title></head>
  <body>
    <h1>No Such Resource</h1>
    <p>host b'<h1>hello there</h1>' not in vhost map</p>
  </body>
</html>
```

This vulnerability was introduced in `f49041b` and first appeared in the 0.9.4 release.

Severity

Low

CVE ID

CVE-2022-39348

Weaknesses

CWE-80