Example Threat Intelligence Report

CVE-2021-41773 – 11th October 2021

Executive Summary

CVE-2021-41773, published 5 October 2021, refers to a vulnerability report concerning a Remote Code Execution (RCE) and Path Traversal flaw in Apache version 2.4.49.

This is a serious vulnerability with exploits observed in the wild well before 5 October. Digital Forensics and Incident Response (DFIR) of affected systems should start as soon as possible.

Senior Decision Maker Recommendations

Incident Response Activities

- Start forensics activities immediately to full determine scope of impact
- Determine whether notifications are necessary

Operational Security Response

- Ensure patching of vulnerable systems takes place as soon as possible
- Consider limiting network exposure of non-critical systems

Threat Detection Response

- Increase alerting of anomalous system log entries
- Increase monitoring of emerging OSINT sources (e.g., Twitter)

Key Findings

- Attackers have gained access to /etc/passwd file on at least one system. This exposes usernames, some group information, and some filesystem path information. It does not expose passwords.
- Apache v2.4.50 is an incomplete fix (see CVE-2021-42013[1]). Recommend updating to v2.4.51.
- If upgrading is not possible, setting the “Require all denied” in the directory permissions of Apache’s configuration will mitigate the threat.
- Exploit attempts against this vulnerability predate the CVE by at least three weeks (logs show mid-September scanning attempts).
- Exploit code is publicly available on Twitter and GitHub, since 5 October

1 https://nvd.nist.gov/vuln/detail/CVE-2021-42013

CVE and Patch Details

On 5 October 2021, CVE-2021-41773 was released[2]. The disclosure details a trivially exploitable vulnerability in Apache v2.4.49, a common web server software package.

Apache Foundation released a patch for v2.4.49 to v2.4.50 on 5 October[3]. This patch from Apache v2.4.49 to v2.4.50 was assessed as an incomplete fix[4] as it did not address a vulnerability that could still be exploited. Any systems that were upgraded to v2.4.50 need to further update to v2.4.51. Additionally, these systems should be checked for signs of exploitation from the vulnerability in v2.4.50.

Exploit Details

The exploit itself is both trivial to perform, and a high-risk situation for any Apache v2.4.49 and v2.4.50 systems. Details on the exploit are available via Twitter and GitHub showing exploitation. To exploit this vulnerability, an attacker only needs to pass a GET request to a vulnerable web server. For example, the below line will grab the /etc/passwd file:

```
GET /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
```

It is possible to exploit this vulnerability using GET requests, POST requests, and likely using other verbs, such as HEAD requests, may result in information disclosure.

This vulnerability can also lead to Remote Code Execution (RCE) for certain strings and in some cases. For example, the below request will result in RCE for vulnerable systems via the execution of the 'id' command:

```
GET /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/bin/sh id
```

The default configuration for Apache v2.4.49 is not vulnerable. The following default configuration settings are needed for the system to not be vulnerable[5]:

```
<Directory />
   Require all denied
</Directory>
```

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

3 https://downloads.apache.org/httpd/CHANGES_2.4

4 https://us-cert.cisa.gov/ncas/current-activity/2021/10/06/apache-releases-security-update-apache-http-server

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

Open Source Intelligence Sources

This vulnerability was extensively covered on social media, and details of the vulnerability and example code are prolific. The below examples reflect some of those findings.

Twitter

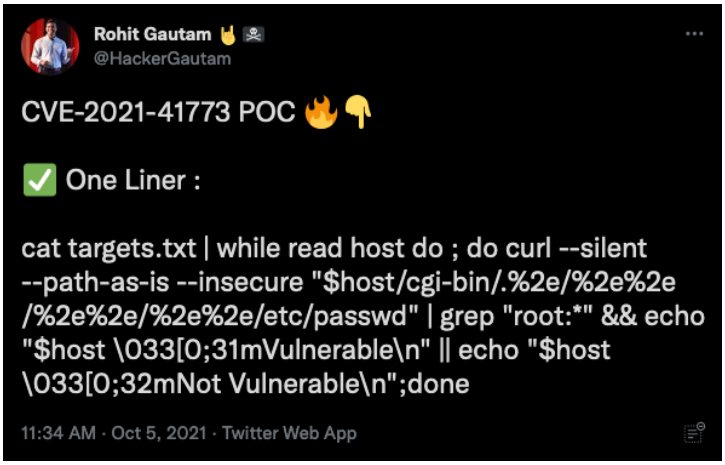

Figure 1 - Tweet showing method to scan hosts and determine vulnerability to CVE-2021-41773

This tweet shows an effective one-line script to scan a list of targets and attempt to fetch the /etc/passwd file off the host. On success, it prints “Vulnerable” and on failure, “Not Vulnerable”. This proves data exfiltration is possible on vulnerable systems using the path traversal bug. This script should not be run against target systems not owned or controlled by the party running the script. Since it uses the vulnerability to exfiltrate data, it may be of questionable legality in some jurisdictions.

The above tweet was published at 11:34 AM (UTC -4) on 05 October 2021. The first public notice of this vulnerability may have been a mailing list post[6] from 09:03:14 UTC on 05 October 2021.

6 https://lists.apache.org/thread.html/r6abf5f2ba6f1aa8b1030f95367aaf17660c4e4c78cb2338aee18982f@%3Cusers.httpd.apache.org%3E

Twitter cont.

Figure 2 - Tweet linking CVE-2021-41773 and CVE-2021-42013

The link from Figure 2 takes us to a short blog post quickly summarizing the state of ongoing scanning of the vulnerability. The commentary is reproduced in full below:

"On October 7, 2021, the Apache Software Foundation released Apache HTTP Server version 2.4.51 to address Path Traversal and Remote Code Execution vulnerabilities (CVE-2021-41773, CVE-2021-42013) in Apache HTTP Server 2.4.49 and 2.4.50. These vulnerabilities have been exploited in the wild.

CISA is also seeing ongoing scanning of vulnerable systems, which is expected to accelerate, likely leading to exploitation. CISA urges organizations to patch immediately if they haven't already—this cannot wait until after the holiday weekend."

Source: https://us-cert.cisa.gov/ncas/current-activity/2021/10/07/apache-releases-http-server-version-2451-address-vulnerabilities

Figure 3 - Tweet showing Shodan search for Apache 2.4.49

Figure 3 shows a screenshot of the total number of vulnerable services globally, as detected by Shodan on 5 October 2021. The significance of the data shows there are possibly 112,758 vulnerable listening service.

Commentary: This exploit saw a lot of coverage on Twitter. The presented tweets only represent a very small fraction of the total coverage. The tweets came very close to the time of the release of the public notices on the vulnerability. The time to Proof of Concept being made public here is very fast. This is typical for this kind of exploit and proves the relevance of using Twitter as an Open Source Intelligence data source for exploits and vulnerabilities data.

GitHub

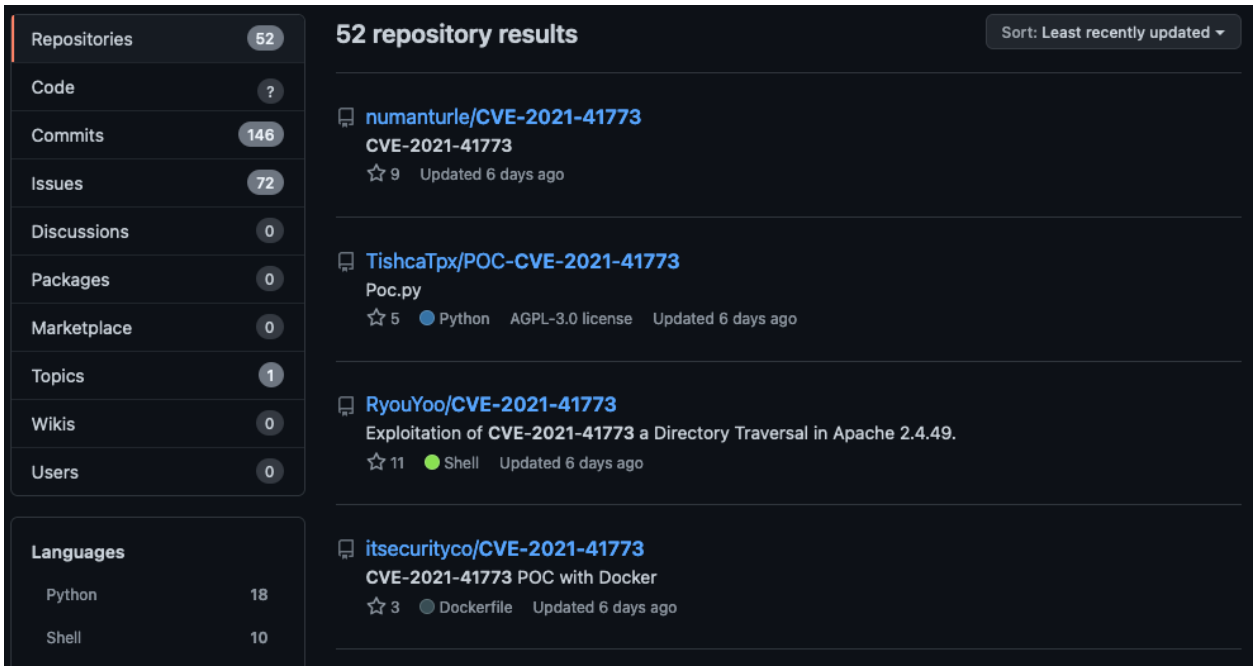

Figure 4 - Shows 52 available GitHub repositories for CVE-2021-41773 on 11 October

GitHub shows many different exploits and scripts in public repos. Our screenshot above shows that there were 52 different repositories that matched “CVE-2021-41773” as a search term. Several projects became available on 5 October.

Commentary: GitHub data does not significantly add to our understanding gained from Twitter. It does serve to confirm the information from Twitter and shows similar short times from vulnerability going public to POC code being available. Some of the projects within GitHub may be useful for scanning our infrastructure to determine our exposure. We should validate the code is benign before relying on any of these tools to use to scan our infrastructure.

Shodan

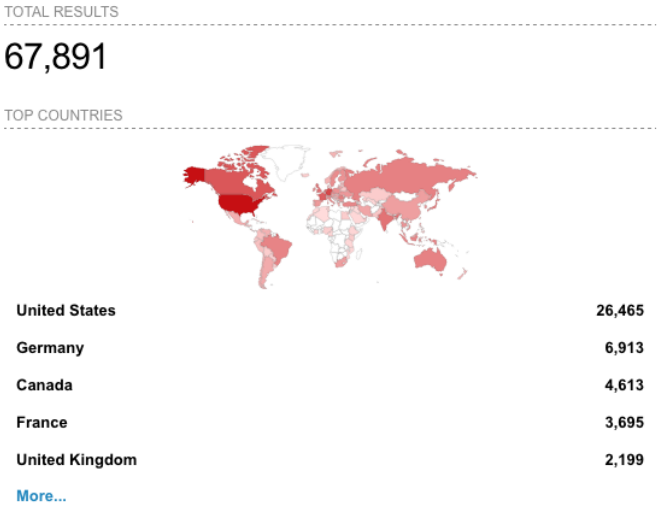

Figure 5 - Shodan search for "Apache/2.4.49" from 11 October

Shodan searches performed on 11 October show 67,891 exposed services reporting themselves to be Apache v2.4.49.

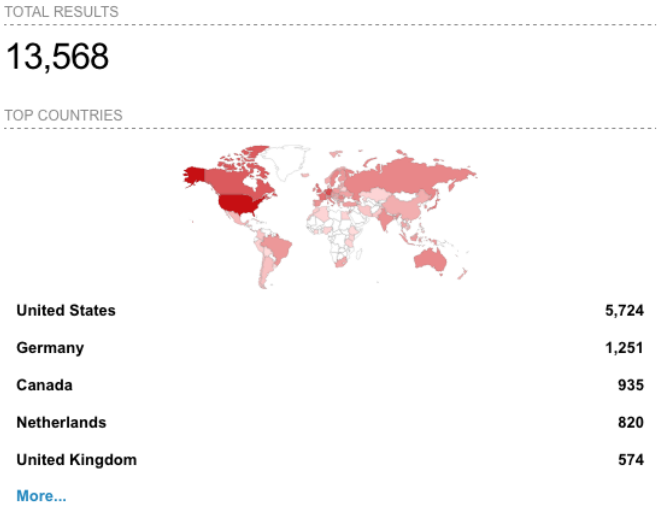

Figure 6 - Shodan search for "Apache/2.4.50" from 11 October

A search for "Apache/2.4.50" performed on 11 October shows 13,568 listening services.

Commentary: Shodan results count each IP and PORT pair as a distinct report for the "Total Results" field. It is common for a single system to run Apache on port 80 and port 443. In some cases, a single system may run Apache on many more ports. This causes the "Total Results" to be larger than the unique host count.
The version detection can be suppressed via the apache configuration. This may cause the "Total Results" to undercount the total services listening and running our target versions.

Given these limitations, it is reasonable to estimate that the unique host count may be about 50% of the "Total Results" for this search. Thus, from 11 October, we can estimate there to be approximately 33,500 unique hosts running Apache v2.4.49 and approximately 6,750 running Apache v2.4.50.

These systems all represent publicly exposed systems in a state that is trivial to exploit. These may well be used for further malicious use, which is a common outcome for this type of exploit and vulnerability.

System Logs

Our system logs show attempts hitting our servers to exploit this vulnerability. Below is an example snippet of our recent log data, showing the most recent attempts.

```
206.188.197.249 - - [10/Oct/2021:20:29:26 +0000] "GET /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd HTTP/1.1" 200 52322
206.188.197.249 - - [11/Oct/2021:00:15:09 +0000] "GET /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd HTTP/1.1" 200 52322
167.99.133.28 - - [11/Oct/2021:13:32:49 +0000] "GET /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/hosts HTTP/1.1" 200 52322
```

Figure 7 - Log snippet showing recent exploitation attempts that appear successful

The “200 52322” numbers at the end of these lines indicate these attempts to grab /etc/passwd were successful. 200 means the request succeeded. The 52322 is the byte count transferred and it matches what we expect for /etc/passwd.

As part of our log search, we found older log lines matching our pattern:

```
64.39.106.39 - - [18/Sep/2021:00:22:15 +0000] "GET /cgi-bin/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/boot.ini HTTP/1.0" 400 226
64.39.106.39 - - [18/Sep/2021:00:22:16 +0000] "GET /cgi-bin/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd HTTP/1.0" 200 52322
64.39.106.39 - - [18/Sep/2021:00:22:56 +0000] "GET /cgi-bin/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/boot.ini HTTP/1.0" 400 226
```

Figure 8 - Log snippet showing attempts hitting us on September 18

Commentary: These log lines show our systems being scanned for boot.ini files and /etc/passwd files. The log dates are well before the public disclosure of this vulnerability. It is unclear what this scanning means. Like the previous example, the “200 52322” indicates successful fetching of our /etc/passwd file. It is unclear whether this is the earliest known instance of our /etc/passwd file being exfiltrated due to this vulnerability.

Summary and Recommendations

CVE-2021-41773 has impacted our organization and may continue to impact us until we take mitigating steps. Logs show our systems being successfully exploited.

For these assets, we expect data exfiltration or exploitation to have already happened. Immediate efforts to identify, isolate, and mitigate this vulnerability for all Apache v2.4.49 servers is recommended. These servers should be patched to v2.4.51 or later after systems are imaged for the DFIR team. The organization does not appear to have Apache v2.4.50 servers, but should any be found, these need to be upgraded to v2.4.51 or later. If patching must be delayed on these servers, we can mitigate the impact of this vulnerability by setting the “Require all **denied” directive.**

We further recommend full DFIR for hosts vulnerable to this issue. Since RCE is possible, there could be further impact beyond that already noted.