Penetration Testing Results Summary

Prepared For: Express Technologies Ltd
Target: EXPRESSVPN WINDOWS APPLICATIONS
Author: LIM SHAO LOONG
Date: 2024-04-08
Version: 4.0

Contents

1 Document Distribution List

Nettitude	Name	Title
	Lim Shao Loong	Security Consultant
	Sojini Yap	Account Manager
	Joshua Chan	Security Consultant
	Iain Wallace	Principal Security Consultant

ExpressVPN	Name	Title
	Aaron Engel	Chief Information Security Officer
	Brian Schimacher	Offensive Security Manager

2 Revision History

Version	Issue Date	Issued by	Comments
0.1	03 March 2024	Lim Shao Loong	Initial Draft
0.2	05 March 2024	Joshua Chan	Quality Assurance
1.0	06 March 2024	Lim Shao Loong	Final Version
1.1	21 March 2024	Lim Shao Loong	Revised Draft
1.2	28 March 2024	Iain Wallace	Quality Assurance
2.0	01 April 2024	Lim Shao Loong	Final Version
3.0	05 April 2024	Lim Shao Loong	Revised Final Version
4.0	08 April 2024	Lim Shao Loong	Revised Final Version

3 Introduction

In March 2024, Express Technologies Ltd engaged Nettitude to conduct a penetration test on the ExpressVPN Windows Applications. The primary objective of this assessment was to ensure that the DNS leak vulnerability related to the split tunnelling feature found in versions v12.72.0.6 and v10.50.0.2 has been remediated.

The following components were tested as part of the engagement:

Component	Description
ExpressVPN for Windows v12.74.0.19 binaries ExpressVPN for Windows v10.51.0.9 binaries	DNS leak vulnerability related to split tunnelling feature was observed in Windows v12.72.0.6 and v10.50.0.2 binaries. The scope of work is to ensure that the patched binaries v12.74.0.19 and v10.51.0.9 have effectively addressed the DNS leak vulnerability in Windows 10 and 11.

During the period of engagement, the new binaries v12.74.0.19 and v10.51.0.9 were tested and deemed to have effectively addressed the DNS leak vulnerability related to the split tunnelling feature. However, a new vulnerability was observed in the v12.74.0.19 and v10.51.0.9 binaries, and has since been fixed. The patched v10 application (v10.53) is available through a direct download link with split tunnelling disabled, effectively resolving the issue. Additionally, the download option on the ExpressVPN website for v10 is removed, thus decommissioning v10 of the Windows application.

This report will address how Nettitude was able to replicate the DNS leak vulnerability, how the new binaries effectively addressed the issues, and finally, the new vulnerability that was observed during the testing period and its remediation.

4 Analysis: ExpressVPN Windows Applications

The ExpressVPN Windows binaries, versions v12.72.0.6 and v10.50.0.2, were found to be affected by a DNS leak vulnerability related to the split tunnelling feature. The split tunnelling feature allows users to selectively choose which applications go through the VPN route and which do not. However, two specific conditions were identified that trigger the DNS leakage.

The two conditions that trigger the DNS leakage and affected specific versions are outlined below:

First Condition – Other VPN applications were installed on the Windows machine.

- v12.72.0.6
- v10.50.0.2

Second Condition – DNS Resolver Cached.

- v12.72.0.6

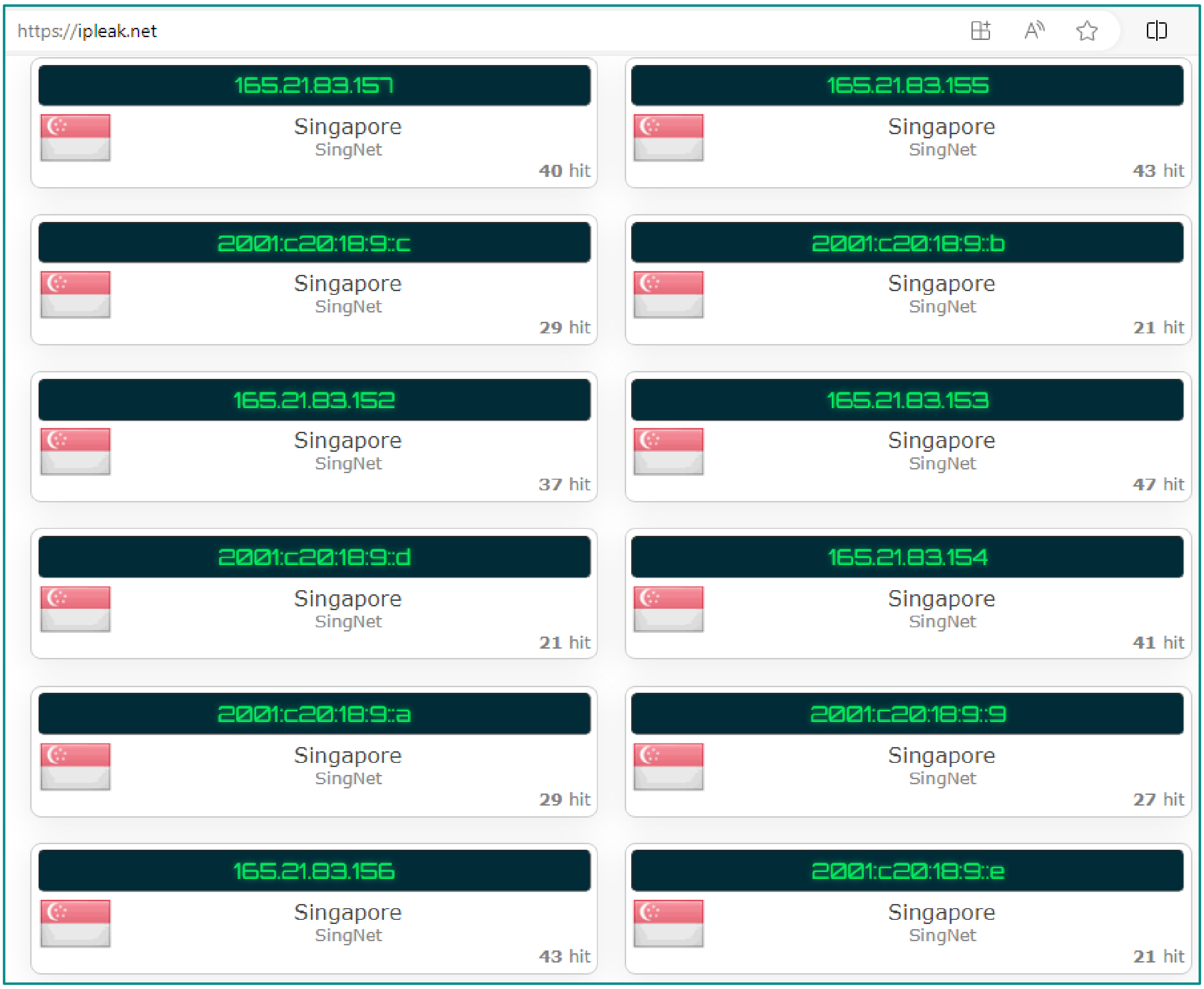
Nettitude then proceeded to replicate the DNS leak vulnerability using the vulnerable versions provided by Express Technologies Ltd.

4.1 Setup of Testing Environment

The following table details the setup of the testing environment for this engagement:

Operating Systems	Applications Installed	ExpressVPN Binaries Tested
Windows 11 (Host Machine), Windows 11 (Virtual Machine)	Google Chrome, NordVPN, IPVanish, SurfShark	v12.72.0.6, v10.50.0.2, v12.74.0.19, v10.51.0.9, v12.75.0.18
Windows 10 (Host Machine), Windows 10 (Virtual Machine)	Google Chrome, NordVPN, IPVanish, SurfShark	v12.72.0.6, v10.50.0.2, v12.74.0.19, v10.51.0.9, v12.75.0.18

The default Internet Service Provider (ISP) used for this engagement is SingNet as shown in the screenshot below:



https://ipleak.net

165.21.83.157
Singapore
SingNet
40 hit

165.21.83.155
Singapore
SingNet
43 hit

2001:c20:18:9::c
Singapore
SingNet
29 hit

2001:c20:18:9::b
Singapore
SingNet
21 hit

165.21.83.152
Singapore
SingNet
37 hit

165.21.83.153
Singapore
SingNet
47 hit

2001:c20:18:9::d
Singapore
SingNet
21 hit

165.21.83.154
Singapore
SingNet
41 hit

2001:c20:18:9::a
Singapore
SingNet
29 hit

2001:c20:18:9::9
Singapore
SingNet
27 hit

165.21.83.156
Singapore
SingNet
43 hit

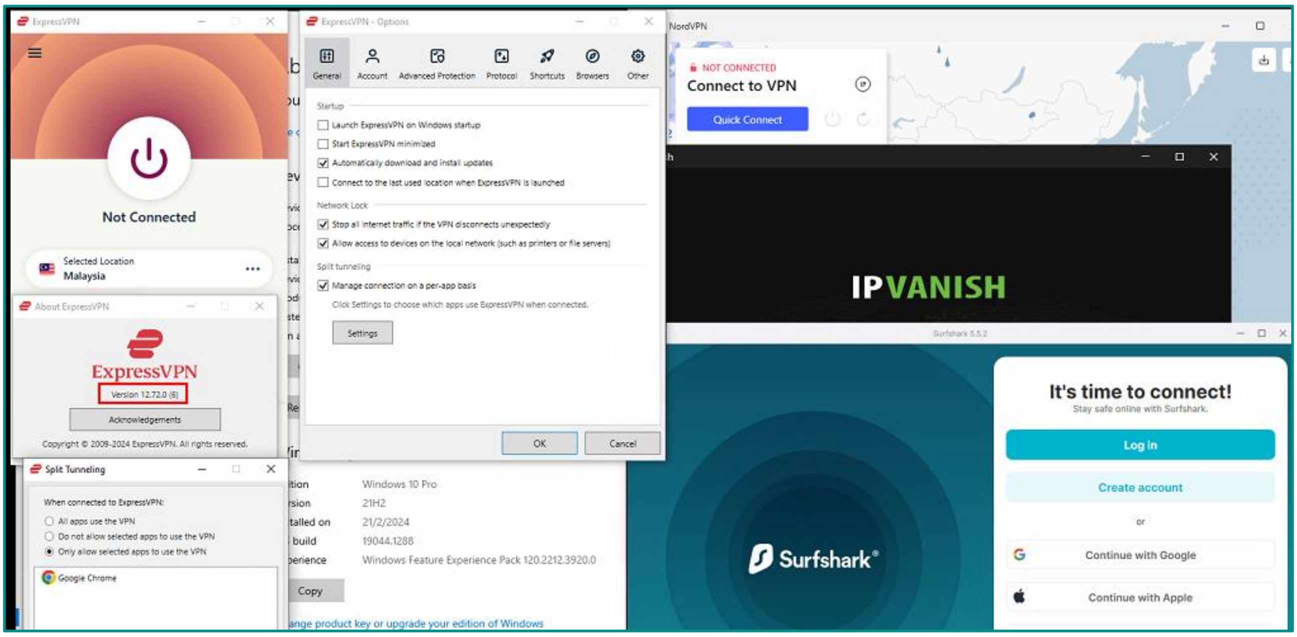
2001:c20:18:9::e
Singapore
SingNet
21 hit

Figure 1: Default ISP, DNS result from ipleak.net.

4.2 Replication of the DNS Leak Vulnerability

4.2.1 First Condition – Other VPN Applications Installed

The following screenshots demonstrate the first condition (Other VPN Applications Installed) to trigger the DNS leak vulnerability:



ExpressVPN

Not Connected

Selected Location: Malaysia

About ExpressVPN

ExpressVPN Version 12.72.0 (6)

Copyright © 2009-2024 ExpressVPN. All rights reserved.

ExpressVPN - Options

Startup
- ☐ Launch ExpressVPN on Windows startup
- ☐ Start ExpressVPN minimized
- ☑ Automatically download and install updates
- ☐ Connect to the last used location when ExpressVPN is launched

Network Lock
- ☑ Stop all internet traffic if the VPN disconnects unexpectedly
- ☑ Allow access to devices on the local network (such as printers or file servers)

Split tunneling
- ☑ Manage connection on a per-app basis

Click Settings to choose which apps use ExpressVPN when connected.

Split Tunneling

When connected to ExpressVPN:
- ○ All apps use the VPN
- ○ Do not allow selected apps to use the VPN
- ● Only allow selected apps to use the VPN

Google Chrome

ition	Windows 10 Pro
rsion	21H2
talled on	21/2/2024
build	19044.1288
perience	Windows Feature Experience Pack 120.2212.3920.0

NordVPN

NOT CONNECTED

Connect to VPN

It's time to connect!

Stay safe online with Surfshark.

Figure 2: Vulnerable v12.72.0.6 and other VPN applications installed with split tunnelling turned on.

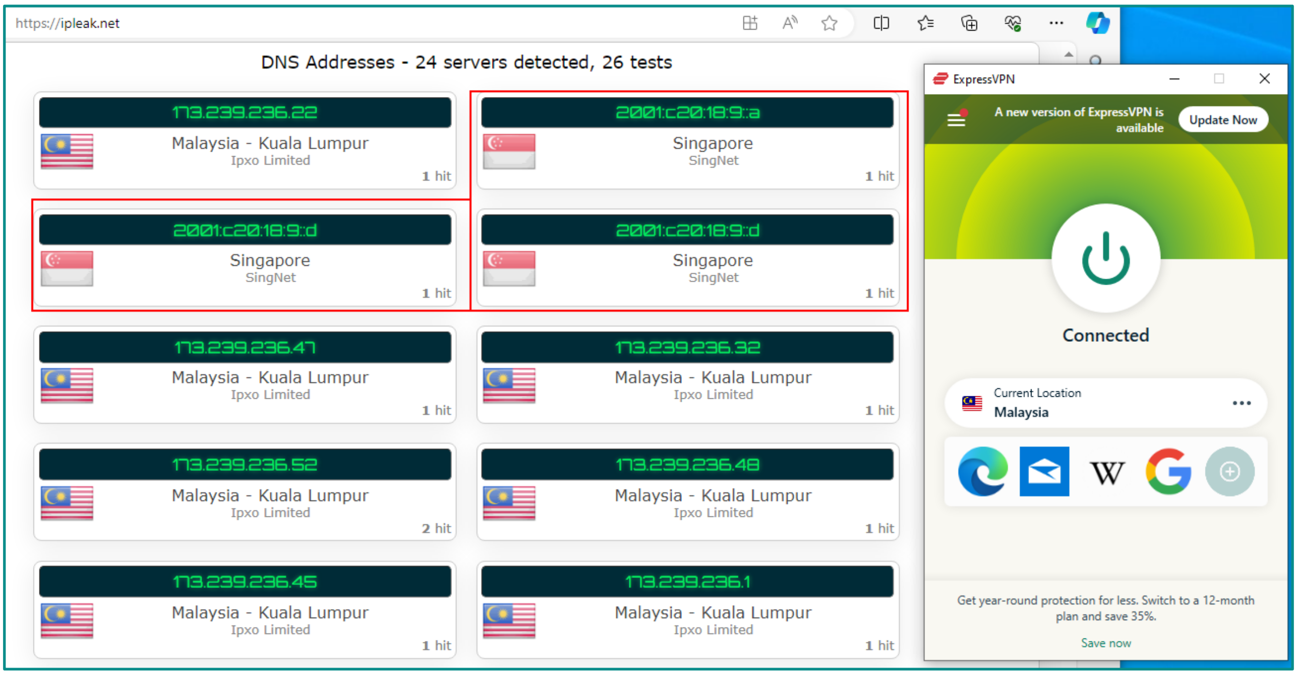
The screenshot above provide details of the setup process for triggering a DNS leak. The ExpressVPN application, along with other VPN applications (namely NordVPN, IPVanish, and Surfshark), were installed on both Windows 10 and Windows 11 systems.

All the setups mentioned are configured with the same split tunnelling feature enabled with “Google Chrome” selected as the application to route through the VPN.

The identical setup and testing environment were also applied to the vulnerable v10.50.0.2 version of the ExpressVPN application. The presence of the other VPN applications listed in this report, when installed on the same machine, consistently triggered the DNS leak issue without any additional actions required beyond installation.

It’s noteworthy that, during testing, some systems experienced a DNS leak with only one of the other VPN applications installed.

After connecting to the ExpressVPN application with split tunnelling enabled, a DNS leak occurred where the service provider (SingNet) is still present in the DNS server list, as shown below:



https://ipleak.net

DNS Addresses - 24 servers detected, 26 tests

173.239.236.22
Malaysia - Kuala Lumpur
Ipxo Limited
1 hit

2001:c20:18:9::a
Singapore
SingNet
1 hit

2001:c20:18:9::d
Singapore
SingNet
1 hit

2001:c20:18:9::d
Singapore
SingNet
1 hit

173.239.236.47
Malaysia - Kuala Lumpur
Ipxo Limited
1 hit

173.239.236.32
Malaysia - Kuala Lumpur
Ipxo Limited
1 hit

173.239.236.52
Malaysia - Kuala Lumpur
Ipxo Limited
2 hit

173.239.236.48
Malaysia - Kuala Lumpur
Ipxo Limited
1 hit

173.239.236.45
Malaysia - Kuala Lumpur
Ipxo Limited
1 hit

173.239.236.1
Malaysia - Kuala Lumpur
Ipxo Limited
1 hit

ExpressVPN

A new version of ExpressVPN is available

Update Now

Connected

Current Location
Malaysia

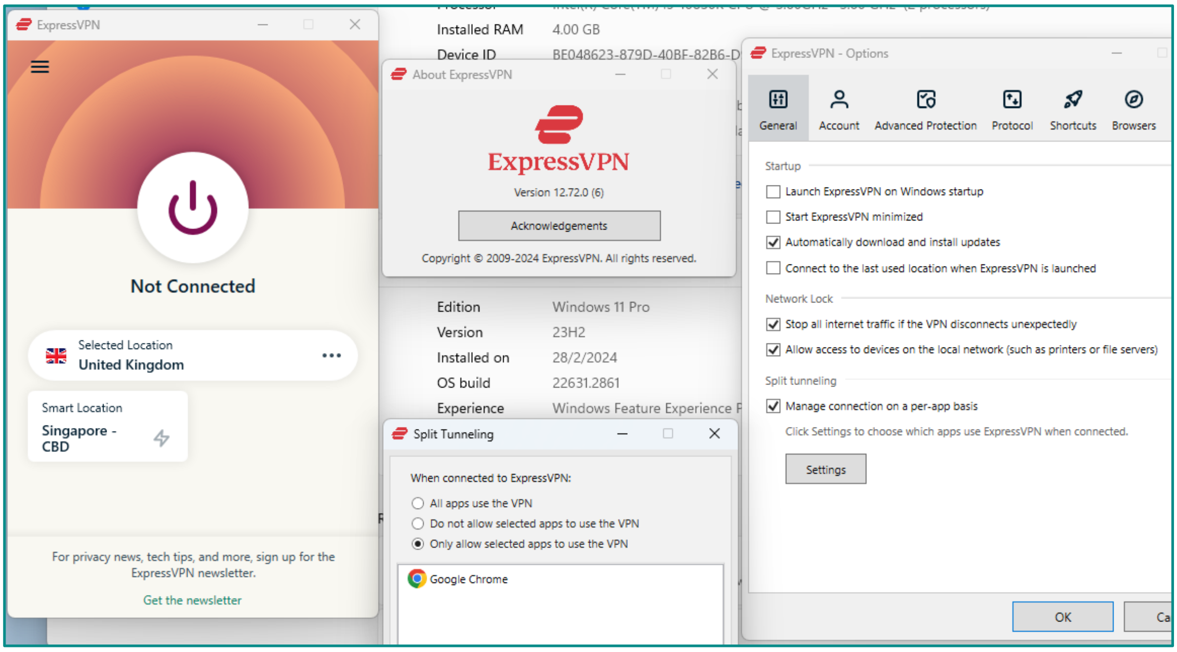
Get year-round protection for less. Switch to a 12-month plan and save 35%.

Save now

Figure 3: DNS leak occurred.

4.2.2 Second Condition – DNS Resolver Cached

The following screenshots demonstrate the second condition (DNS Resolver Cached) to trigger the DNS leak vulnerability:



ExpressVPN

Not Connected

Selected Location
United Kingdom

Smart Location
Singapore - CBD

For privacy news, tech tips, and more, sign up for the ExpressVPN newsletter.

Get the newsletter

Installed RAM 4.00 GB
Device ID BE048623-879D-40BF-82B6-D

About ExpressVPN

ExpressVPN
Version 12.72.0 (6)

Acknowledgements

Copyright © 2009-2024 ExpressVPN. All rights reserved.

Edition Windows 11 Pro
Version 23H2
Installed on 28/2/2024
OS build 22631.2861
Experience Windows Feature Experience P

Split Tunneling

When connected to ExpressVPN:

○ All apps use the VPN
○ Do not allow selected apps to use the VPN
● Only allow selected apps to use the VPN

Google Chrome

ExpressVPN - Options

General | Account | Advanced Protection | Protocol | Shortcuts | Browsers

Startup

□ Launch ExpressVPN on Windows startup
□ Start ExpressVPN minimized
☑ Automatically download and install updates
□ Connect to the last used location when ExpressVPN is launched

Network Lock

☑ Stop all internet traffic if the VPN disconnects unexpectedly
☑ Allow access to devices on the local network (such as printers or file servers)

Split tunneling

☑ Manage connection on a per-app basis

Click Settings to choose which apps use ExpressVPN when connected.

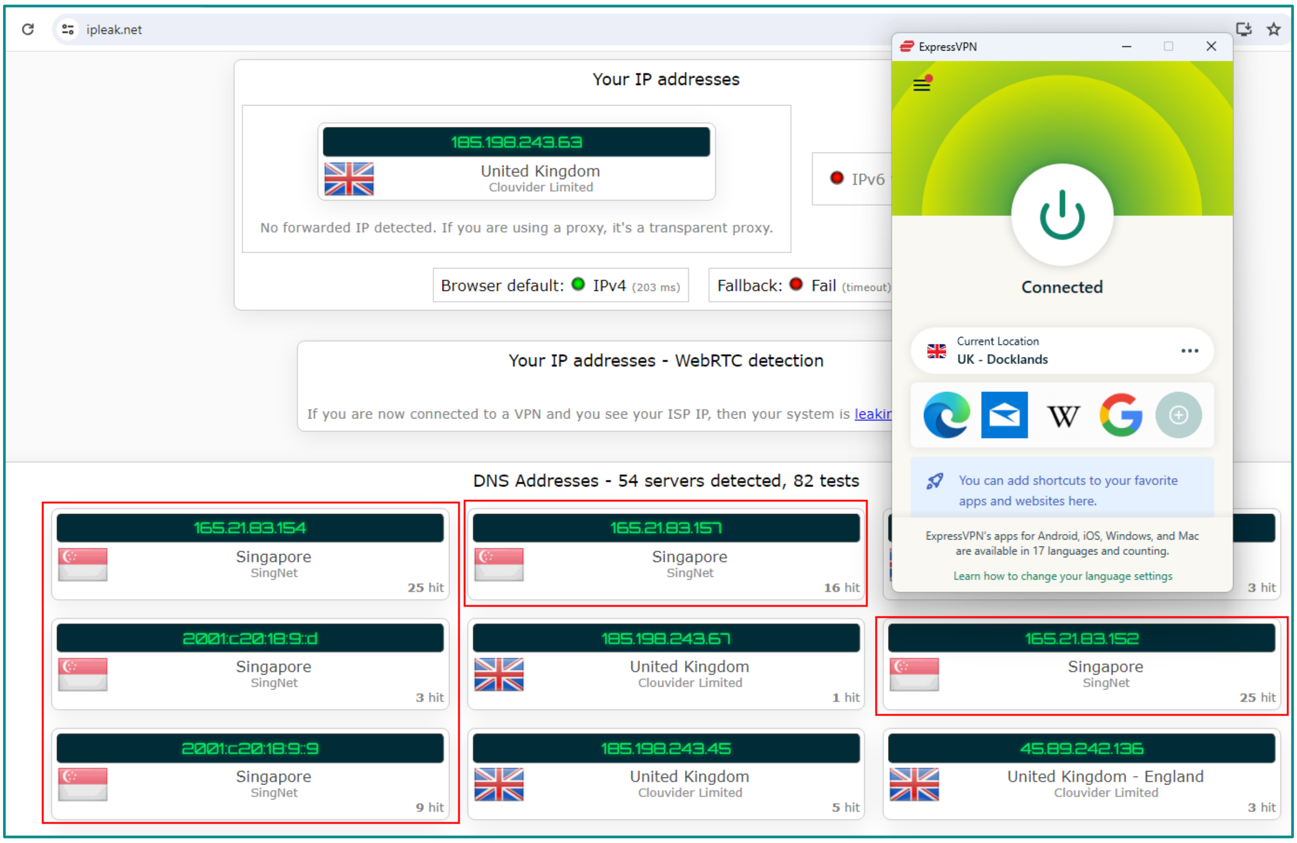
Settings

OK | Ca

Figure 4: Vulnerable v12.72.0.6 application installed with split tunnelling turned on.

The DNS leak based on the second condition was triggered by implementing the same setup as the first condition, excluding other VPN applications that were installed.

Nettitude then proceeded to perform several DNS queries to ensure the DNS resolver was cached. This can be achieved through dnsleaktest.com. Following this, connecting to a VPN profile that is geographically distant from the current location resulted in the DNS leak illustrated below.



ipleak.net

Your IP addresses

185.198.243.63
United Kingdom
Clouvider Limited

No forwarded IP detected. If you are using a proxy, it's a transparent proxy.

● IPv6

Browser default: ● IPv4 (203 ms)

Fallback: ● Fail (timeout)

Your IP addresses - WebRTC detection

If you are now connected to a VPN and you see your ISP IP, then your system is leakir

DNS Addresses - 54 servers detected, 82 tests

165.21.83.154 Singapore SingNet 25 hit	165.21.83.157 Singapore SingNet 16 hit	3 hit
2001:c20:18:9::d Singapore SingNet 3 hit	185.198.243.67 United Kingdom Clouvider Limited 1 hit	165.21.83.152 Singapore SingNet 25 hit
2001:c20:18:9::9 Singapore SingNet 9 hit	185.198.243.45 United Kingdom Clouvider Limited 5 hit	45.89.242.136 United Kingdom - England Clouvider Limited 3 hit

ExpressVPN

Connected

Current Location
UK - Docklands

You can add shortcuts to your favorite apps and websites here.

ExpressVPN's apps for Android, iOS, Windows, and Mac are available in 17 languages and counting.

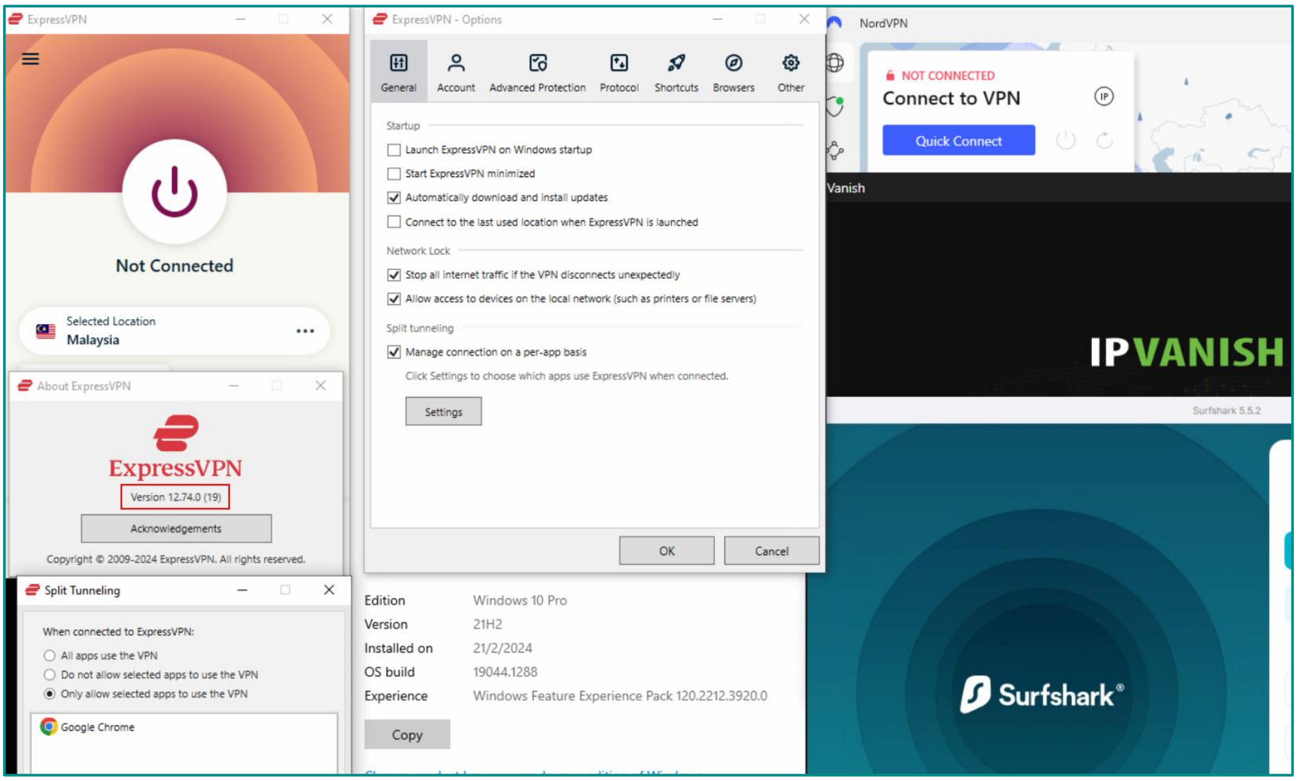
Learn how to change your language settings

Figure 5: DNS leakage observed from ipleak.net results.

4.3 Remediation of the DNS Leak Vulnerability

During the testing period, the tested application versions v12.74.0.9 and v10.51.0.9 successfully resolved the DNS leakage, as shown below:

4.3.1 First Condition – Other VPN Applications Installed (Remediated)



Version 12.74.0 (19)

Copyright © 2009-2024 ExpressVPN. All rights reserved.

Startup

□ Launch ExpressVPN on Windows startup

□ Start ExpressVPN minimized

☑ Automatically download and install updates

□ Connect to the last used location when ExpressVPN is launched

Network Lock

☑ Stop all internet traffic if the VPN disconnects unexpectedly

☑ Allow access to devices on the local network (such as printers or file servers)

Split tunneling

☑ Manage connection on a per-app basis

Click Settings to choose which apps use ExpressVPN when connected.

When connected to ExpressVPN:

○ All apps use the VPN

○ Do not allow selected apps to use the VPN

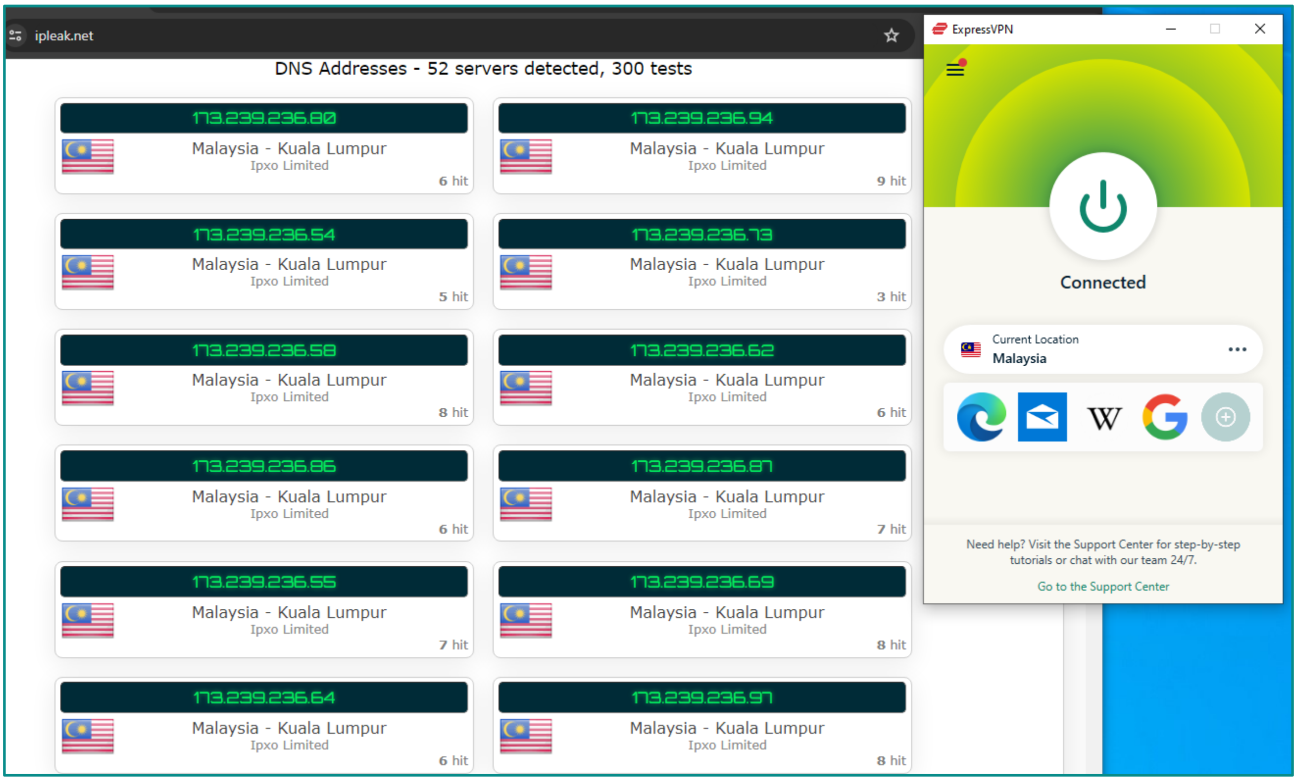
● Only allow selected apps to use the VPN

Google Chrome

Edition	Windows 10 Pro
Version	21H2
Installed on	21/2/2024
OS build	19044.1288
Experience	Windows Feature Experience Pack 120.2212.3920.0

Figure 6: Patched v12.74.0.19 and other VPN applications installed with split tunnelling turned on.

Nettitude performed the same tests on the new binaries using the setup detailed in section 4.2.1, utilizing several DNS leak tools (such as ipleak.net and dnsleaktest.com) to ensure that the issue was resolved. The initial DNS leak vulnerability triggered by the first condition – "other competing VPN applications installed" were deemed to have been effectively remediated by the new binaries v12.74.0.19 and v10.51.0.9.



ipleak.net

DNS Addresses - 52 servers detected, 300 tests

173.239.236.80
Malaysia - Kuala Lumpur
Ipxo Limited
6 hit

173.239.236.94
Malaysia - Kuala Lumpur
Ipxo Limited
9 hit

173.239.236.54
Malaysia - Kuala Lumpur
Ipxo Limited
5 hit

173.239.236.73
Malaysia - Kuala Lumpur
Ipxo Limited
3 hit

173.239.236.58
Malaysia - Kuala Lumpur
Ipxo Limited
8 hit

173.239.236.62
Malaysia - Kuala Lumpur
Ipxo Limited
6 hit

173.239.236.86
Malaysia - Kuala Lumpur
Ipxo Limited
6 hit

173.239.236.87
Malaysia - Kuala Lumpur
Ipxo Limited
7 hit

173.239.236.55
Malaysia - Kuala Lumpur
Ipxo Limited
7 hit

173.239.236.69
Malaysia - Kuala Lumpur
Ipxo Limited
8 hit

173.239.236.64
Malaysia - Kuala Lumpur
Ipxo Limited
6 hit

173.239.236.97
Malaysia - Kuala Lumpur
Ipxo Limited
8 hit

ExpressVPN

Connected

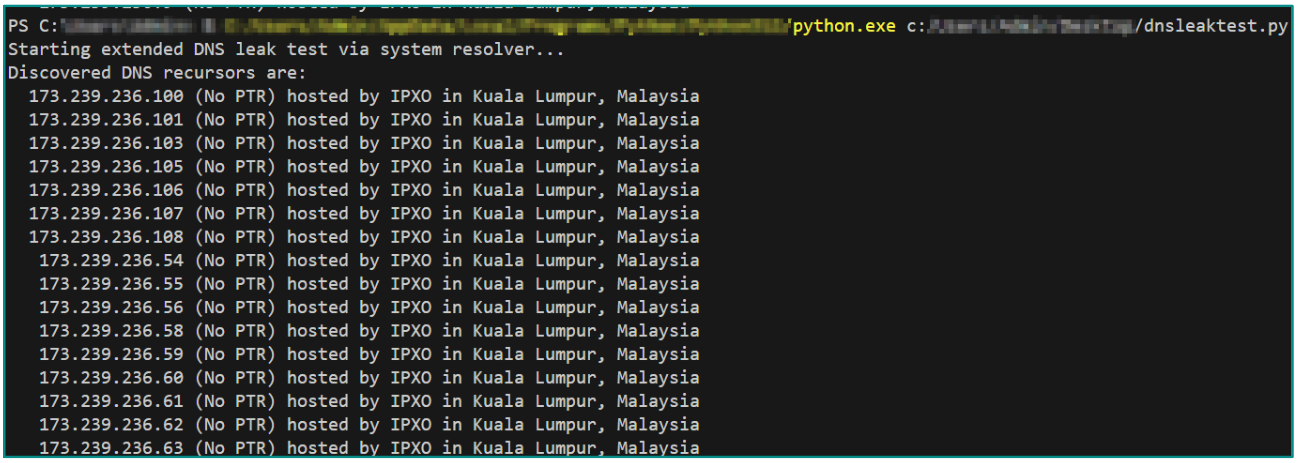
Current Location
Malaysia

Need help? Visit the Support Center for step-by-step tutorials or chat with our team 24/7.

Go to the Support Center

Figure 7: DNS leakage no longer occurs (ipleak.net).

4.3.2 Second Condition – DNS Resolver Cached (Remediated)



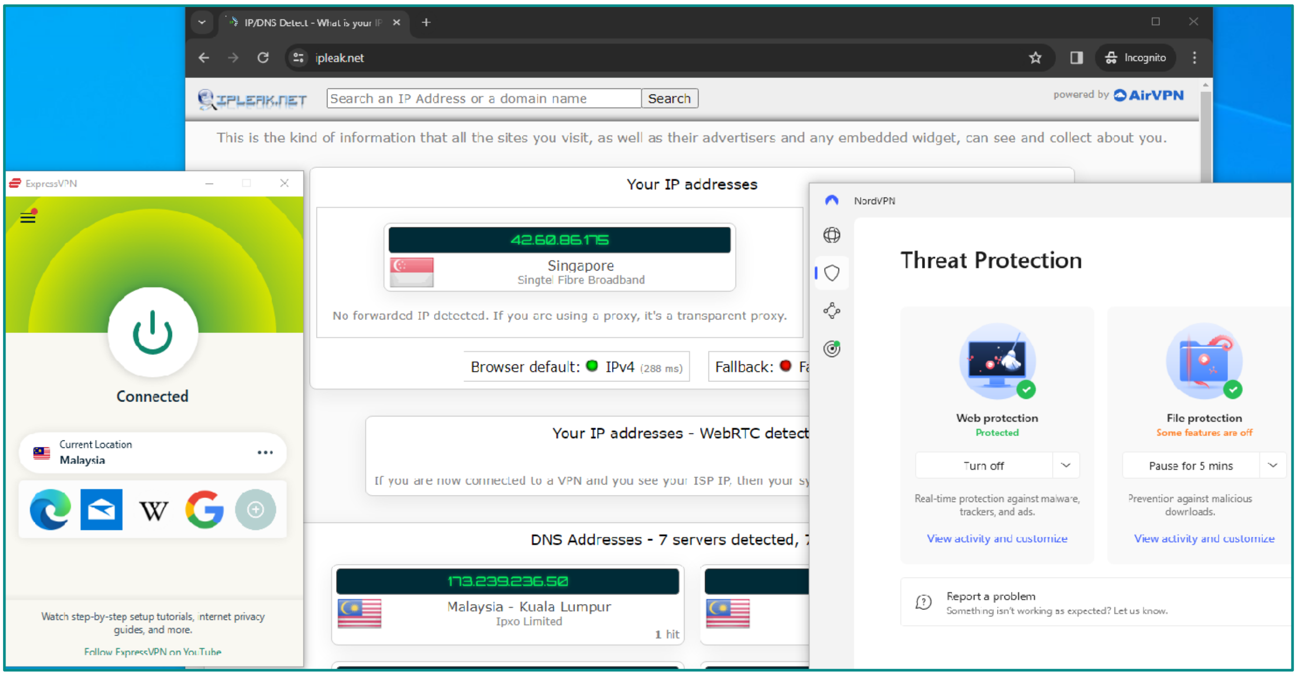
```
PS C:[redacted]python.exe c:[redacted]/dnsleaktest.py
Starting extended DNS leak test via system resolver...
Discovered DNS recursors are:
  173.239.236.100 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
  173.239.236.101 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
  173.239.236.103 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
  173.239.236.105 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
  173.239.236.106 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
  173.239.236.107 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
  173.239.236.108 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
   173.239.236.54 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
   173.239.236.55 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
   173.239.236.56 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
   173.239.236.58 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
   173.239.236.59 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
   173.239.236.60 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
   173.239.236.61 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
   173.239.236.62 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
   173.239.236.63 (No PTR) hosted by IPXO in Kuala Lumpur, Malaysia
```

Figure 8: DNS leakage no longer occurs (dnsleaktest.com).

Nettitude replicated the same tests on the new binary using the setup detailed in section 4.2.2, employing the same tools mentioned above to verify the resolution of the issue. The initial DNS leak vulnerability triggered by the second condition, DNS resolver cached issue, was determined to have been effectively remediated by the new binary v12.74.0.19.

4.4 IP Leak and Misconfigured VPN Profile

While the DNS leak issue was resolved, it was observed that the patched ExpressVPN application v12.74.0.19 and v10.51.0.9 binaries introduced another bug, leading to the leakage of the ISP's IP or being assigned to a misconfigured VPN profile for browser applications as shown in the screenshots below:



This is the kind of information that all the sites you visit, as well as their advertisers and any embedded widget, can see and collect about you.

Your IP addresses

42.60.86.175
Singapore
Singtel Fibre Broadband

No forwarded IP detected. If you are using a proxy, it's a transparent proxy.

Browser default: ● IPv4 (288 ms) Fallback: ● Fa

Your IP addresses - WebRTC detect

If you are now connected to a VPN and you see your ISP IP, then your sy

DNS Addresses - 7 servers detected, 7

173.239.236.50
Malaysia - Kuala Lumpur
Ipxo Limited
1 hit

Connected

Current Location
Malaysia

Watch step-by-step setup tutorials, internet privacy guides, and more.

Follow ExpressVPN on YouTube

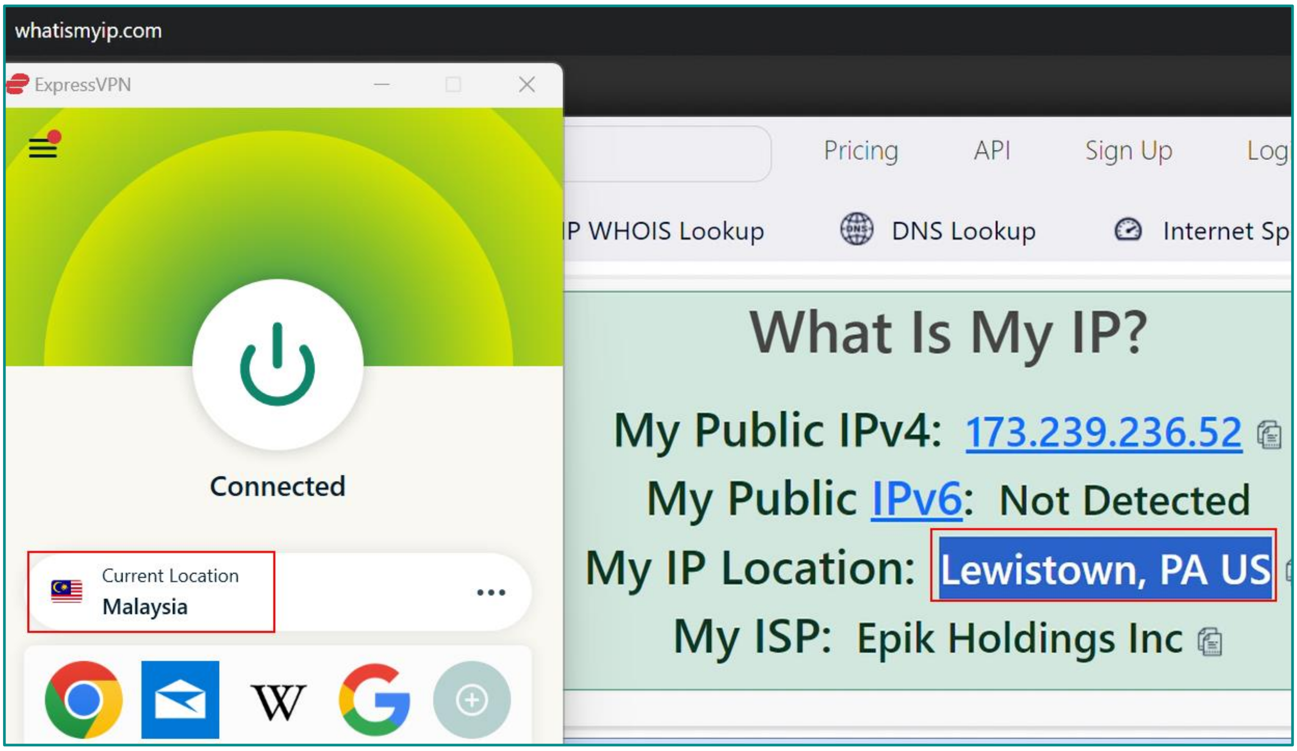
Threat Protection

Web protection
Protected
Turn off
Real-time protection against malware, trackers, and ads.
View activity and customize

File protection
Some features are off
Pause for 5 mins
Prevention against malicious downloads.
View activity and customize

Report a problem
Something isn't working as expected? Let us know.

Figure 9: ISP's IP was leaked through the patched applications (Virtual Machine).



Connected

Current Location
Malaysia

What Is My IP?

My Public IPv4: 173.239.236.52

My Public IPv6: Not Detected

My IP Location: Lewistown, PA US

My ISP: Epik Holdings Inc

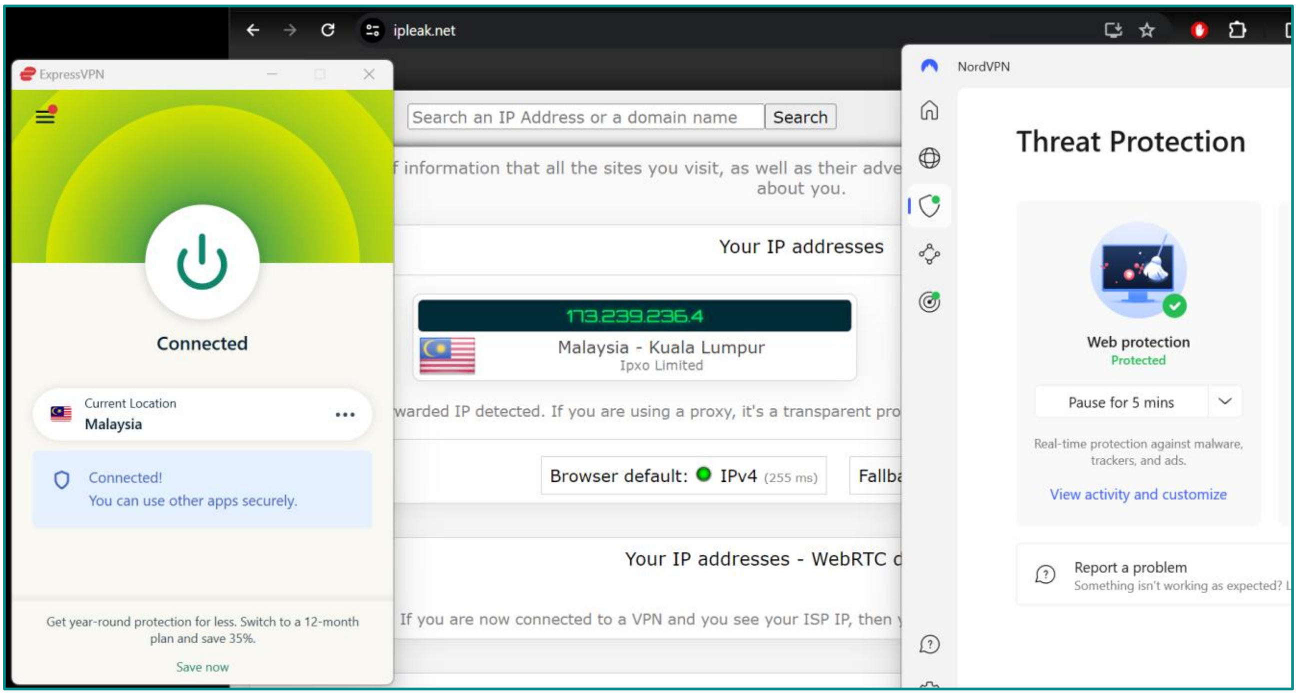
Figure 10: Incorrect VPN profile assigned through the patched applications (Physical Host Machine).

The newly identified issue was reported to the respective teams, and it was quickly narrowed down. The team released a newly patched application, v12.75.0.18, to address the issue, and a retest confirmed its successful remediation.

The patched v10 application (v10.53) is available through a direct download link with split tunnelling disabled, effectively resolving the issue. Additionally, the download option on the ExpressVPN website for v10 is removed, thus decommissioning v10 of the Windows application.

The newly identified issue stemmed from NordVPN's Threat Protection (Web Protection) feature (left in its default state after installation), which either displayed a misconfigured VPN profile or leaked the ISP's IP address, depending on whether the machine used was virtual or physical, within the split tunnelling feature.

The following screenshots depict that the issue has been remediated:



Connected

Current Location
Malaysia

Connected!
You can use other apps securely.

Get year-round protection for less. Switch to a 12-month plan and save 35%.

f information that all the sites you visit, as well as their adve
about you.

Your IP addresses

173.239.236.4
Malaysia - Kuala Lumpur
Ipxo Limited

warded IP detected. If you are using a proxy, it's a transparent pro

Browser default: ● IPv4 (255 ms) Fallba

Your IP addresses - WebRTC d

If you are now connected to a VPN and you see your ISP IP, then y

Threat Protection

Web protection
Protected

Real-time protection against malware, trackers, and ads.

View activity and customize

Report a problem
Something isn't working as expected? L

Figure 11: Correct VPN profile is now assigned with NordVPN's Web Protection

5 Overview of Findings

5.1 Finding Summary

Nettitude identified a total number of one finding during the engagement. The following table shows the categorisation by severity:

0	0	1	0	0
Critical	High	Medium	Low	Info.

5.2 ExpressVPN Windows Applications Summary

Component	Description	Status
v12.74.0.19, v10.51.0.9	DNS Leak Vulnerability	Remediated
V12.75.0.18	IP Leak and Misconfigured VPN Profile	Remediated
v10.x	IP Leak and Misconfigured VPN Profile	Decommissioned due to removal of split tunnelling in v10.53

CREST

VA | PEN TEST | STAR Intelligence-led PT | STAR Threat intelligence | CSIR | SOC | OVS

PCI Security Standards Council™ QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council™ APPROVED SCANNING VENDOR

CYBER ESSENTIALS

bsi ISO 9001 Quality Management Systems CERTIFIED

ISO/IEC 27001 Information Security Management CERTIFIED

ISO 14001:2004 REGISTERED FIRM

Get in touch

Visit **www.nettitude.com** for more information
or email enquiries to **solutions@nettitude.com**

UK Head Office
1 Trinity Park
Bickenhill Ln
Birmingham
B37 7ES

Americas
810 Seventh Av
Suite 1110
New York
NY 10019

Asia Pacific
460 Alexandra Rd
#15-01
mTower
Singapore 119963

Europe
Fidiou 9
Athina
106 78
Greece

LRQA NETTITUDE