

SECURITY ASSESSMENT OF EXPRESSVPN WINDOWS APPLICATION (V12)

ExpressVPN

2022-04-21

Project Team

Assessment Team

Lead Consultant	Ritchie Fergindo
-----------------	------------------

Quality Assurance

Document QA	Wong Cheng-Teck
Document Technical QA	Sven Schleier



Contents

1	EXECUTIVE SUMMARY	4
2	APPROACH, FINDINGS AND RECOMMENDATIONS	6
3	SUMMARY OF VULNERABILITIES	10
3.1	Total Vulnerabilities Found During this Test	10
3.2	Summary of Vulnerabilities Found	10
4	WINDOWS APPLICATION ASSESSMENT VULNERABILITIES.....	11

1 Executive Summary

F-Secure Consulting was engaged by ExpressVPN to conduct a penetration test targeting the ExpressVPN Windows Application (v12).

The scope of the penetration test was to conduct a “White-box” Windows Application security assessment targeting the ExpressVPN Windows Application (v12) within the Production environment for 17 man-days (inclusive of reporting) between 7 February 2022 and 2 March 2022.

ExpressVPN Windows (v12) was used at the time of writing as the new primary client for Windows users. It provides connection via various VPN protocols to the ExpressVPN service on the Windows platform.

The purpose of the assessment was to identify security weaknesses within the ExpressVPN Windows Application (v12) that could be exploited by an adversary to affect the confidentiality, integrity or availability of systems or data, or which could be used to cause significant reputational damage to ExpressVPN.

The main objectives of this assessment were to identify vulnerabilities relating to:

1. Information disclosure or IP address leakage
2. Remote code execution (RCE)

While the assessment was performed using a “White-Box” methodology, a “Grey-Box” approach was also used to evaluate components with no source code provided. To elaborate: F-Secure Consulting was provided with the debug production build which facilitated testing, and the testing/development tools were out of scope.

The assessment was conducted from F-Secure Consulting’s Singapore office, by the F-Secure Consulting Singapore offensive security team.

The approach to testing was conducted in line with accepted industry standards, such as Open-Source Security Testing Methodology Manual (OSSTMM), Open Web Application Security Project (OWASP), CREST, and the CHECK guidelines produced by NCSC for testing UK Government protectively marked systems and networks.

The severity ratings used within this report are based on the Common Vulnerability Scoring System version 3 (CVSSv3).

The CVSSv3 calculations do not include Environmental Metrics which cannot be quantified or tested based on penetration testing alone, and which should be completed by the internal risk management function.

It is recommended that an internal risk analysis of the findings in this report be conducted to account for internal compensating controls, environmental factors, and business impact.

The results of this analysis will enable the Environmental Metrics calculation to be applied to the CVSSv3 score and incorporated into the risk register to derive the residual risk, enabling contextual risk treatment decisions to be taken by the risk owner.

During the assessment, no issues of Critical, High, Medium, or Low were discovered, only one (1) Informational observation. There were no vulnerabilities identified which would directly result in arbitrary code execution and information disclosure or IP address leakage. Below is the finding identified during this assessment:

- The application was observed to use insecure C/C++ functions. However, it was confirmed that the usage of these functions was not exploitable because manual buffer checks, guaranteed sizes, and proper null termination were implemented on the insecure C/C++ functions to prevent memory corruption attacks. This issue was raised as deviation from best practices.

In summary, F-Secure did not identify vulnerabilities which can be exploited to cause information disclosure, IP address leakage or RCE in the ExpressVPN Windows application.

Retest Status (2022-04-13)

A retest assessment of the following one (1) issue was conducted on 13 April 2022 against the ExpressVPN Windows Application (v12) version 12.21.0.25. The following is a summary of the retest status for the issue.

Windows Application Assessment Vulnerabilities

- Insecure Function Used – **Closed**

2 Approach, Findings and Recommendations

Overview

This section of the report discusses the main issues that were discovered together with high level recommendations as to how they may be best resolved. Further detail on individual issues together with specific technical recommendations are given in Section 6 of this report.

The purpose of this engagement was to verify that security controls were effective against prevailing threats and vulnerabilities, through the identification of security weaknesses. Technical recommendations were also provided to ExpressVPN to eliminate or mitigate the identified risks.

The objective of the security assessment is outlined below:

- Identify security weaknesses that could be leveraged by an attacker to access or modify sensitive data or assets, cause disruption to service, or which could compromise user's privacy as a result of installing the ExpressVPN Windows application.
- Provide ExpressVPN with assurances with regards to the security posture of the in-scope application.
- Highlight areas where improvements could be made to reduce the risk of a security incident occurring, thereby helping to ensure the confidentiality, integrity, and availability of systems and data belonging to ExpressVPN or their clients.

ExpressVPN Windows v12 was used at the time of writing as one of the available ExpressVPN clients for Windows. It allows the client to connect via various VPN protocols to the ExpressVPN service on the Windows platform. In this assessment, the client application and its components, together with the various VPN protocols, were audited for vulnerabilities.

The protocols supported are listed below:

- Lightway (UDP and TCP)
- OpenVPN (UDP and TCP)

The VPN configuration files and connections set up using the above protocols were reviewed for vulnerabilities that may expose information or compromise user privacy. The protocols themselves were not assessed during the time-boxed assessment but the manner in which these protocols were used during VPN usage, including the connection setup that may expose information or compromise user privacy. The API servers (AWS), as well as the VPN servers itself, were out of scope of the assessment, were out of scope of the assessment. However, traffic to/from the VPN servers was still considered in scope.

Windows Application Security Assessment

The ExpressVPN Windows application (`ExpressVPN.exe`) entails a minimal user interface design and does not require elevated privileges to run. Users may choose from a predefined list of countries and protocols for the VPN connection.

In a similar manner to the ExpressVPN Windows application, the ExpressVPN Notifications Service (`ExpressVPNNotificationService.exe`) runs without elevated privileges.

Application Service Core

The ExpressVPN Application Service Core (`ExpressVPN.AppService.exe`) was a low privileged Local Service application responsible for instrumenting app flows with higher privileged services.

The ExpressVPN Application Service Core offered a gRPC server on local interface on port 2022. Traffic between the client and this gRPC server was observed to be encrypted with TLS 1.2.

The Application Service Core was observed to not directly accept user input and no misconfiguration was identified that could be used to spawn arbitrary elevated processes. The Application Service Core was also observed to not write data that may compromise user privacy to log files.

Browser Extension Helper

The ExpressVPN Browser Extension Helper (`ExpressVPN.BrowserHelper.exe`) supports interaction with the VPN through a browser extension. The extension entails a minimal user interface design and does not require elevated privileges to run. Users may choose from a predefined list of countries and protocols for the VPN connection. Free-form inputs such as website links for shortcuts and file paths were properly validated and launched with the same privileges as the parent process.

The ExpressVPN Browser Extension communicated with the Application Service Core through the gRPC protocol. The traffic was observed to be encrypted with TLS 1.2.

The `manifest.json` for both Chrome and Firefox extensions were assessed. The `externally_connectable` manifest property was observed to be disabled by default. In addition, "Allow access to file URLs" and "collect errors" permissions were also observed to be disabled by default. Thus, this configuration is consistent with the principle of least privilege for permissions.

From `manifest.json`, it was also observed that files under `web_accessible_resources` were not susceptible to clickjacking attacks. Attempts to embed the file directly was unsuccessful.

The browser extension was observed to not accept arbitrary user input, thus eliminating the possibilities of reflected XSS or HTML injection.

Lastly, the ExpressVPN Browser Extension config and log files were observed to not write data to log files that may compromise user privacy.

VPN Service Core

The ExpressVPN VPN Service Core (`ExpressVPN.VpnService.exe`) supported the VPN connection.

The VPN's configuration data were stored securely within `C:/ProgramData/ExpressVPN` directory and requires elevated privileges to access.

ExpressVPN VPN Service Core (`ExpressVPN.VpnService.exe`) would call either `lightway.exe` or `openvpn.exe` with elevated privileges based on the application setting. The path and the executable names to call `lightway.exe` and `openvpn.exe` from `ExpressVPN.AppService.exe` were observed to be hard-coded and no user input was observed to be able to modify these calls. Thus, preventing privilege escalation attacks surface by calling arbitrary executables from `ExpressVPN.AppService.exe`.

It was also observed that the Lightway config files were stored securely within `C:\ProgramData\ExpressVPN\Lightway\Config`. The config files were encrypted using Microsoft DPAPI and would be decrypted by ExpressVPN VPN Service Core (`ExpressVPN.VpnService.exe`) right before `lightway.exe` was called. These config files were decrypted and assessed to find out whether the parameters could be used as attack vector such as arbitrary command execution. However, during the analysis it was observed that the json parameters in the config files were properly validated.

Overall, there were no vulnerabilities identified within the ExpressVPN processes and services which could be exploited by a malicious adversary to execute arbitrary code with elevated privileges during the time-boxed assessment. The Windows service would also start a new process immediately whenever its process had been terminated ungracefully.

Network Traffic

The outgoing traffic from the ExpressVPN client was assessed to ensure there was no sensitive data transmitted in plain text. For this purpose, network sniffers were installed to capture and monitor outbound traffic from the computer where ExpressVPN client was installed. From the captured outbound traffic, computer Network communication to the VPN servers were observed to be encrypted, in line with security best practices.

For the Lightway protocol, the data was transmitting securely with the support of AES or ChaCha20 encryption. In addition, it was also observed to be running on TLS 1.3 over TCP.

Similarly, the configuration defined in `config.vpn` for the OpenVPN protocol was also securely configured, and in line with security best practices. These practices include the use of keys and certificates generated using at least 2048 bits and using TLS 1.2 at the minimum.

It was not possible to gain information about ExpressVPN's clients or out of the network traffic. Nor was it possible to execute code remotely through attacks such as Man-in-the-Middle (MitM), TLS downgrading or packet injection. Attempts to prompt conditions that could initiate IP Address/DNS Leakage such as making DNS requests outside the VPN tunnel or forcefully terminate the running tunnel were conducted. When the VPN service was running, any DNS requests outside the VPN tunnel were unsuccessful. It was also observed when the VPN tunnel was terminated forcefully or there was a switch or outage of the connections, a network lock mechanism was initiated to prevent possible IP Address or DNS information Leakage.

Storage

The ExpressVPN installer required administrative privileges to run but provided no avenues for privilege escalation attacks. Users were limited to clicking the "Install" button to complete the full installation process; the installer provided no other options for users to configure (e.g. installation path).

The files and folders in the default installation and `ProgramData` directories were also found to be securely configured and did not provide any privilege escalation vectors.

Source Code Review

The source code in the following repositories were reviewed under time-boxed conditions:

- **xv_helium_cli (Lightway)**
 - The connector that allows Lightway to be used as a VPN protocol
- **xv_proteus**
 - Main logic that handles connections and application functionality
- **xv_win_v4**
 - Main Windows application code; handles setup and installation

F-Secure Consulting placed emphasis on code within `src`, `drivers`, and directories as highlighted by ExpressVPN. Third-party libraries, dependencies, development/testing tools and files labelled for non-Windows Operating Systems were considered out of scope.

C and C++ functions which does not safely validate user inputs were found to be used within the `xv_helium_cli` repository. It was confirmed that the usage of these functions was not exploitable as manual buffer size checks, guaranteed sizes and proper null termination were observed to be implemented on the applications.

3 Summary of Vulnerabilities

3.1 Total Vulnerabilities Found During this Test

The following table presents the total number of vulnerabilities discovered during testing, by severity.

Scope	CRITICAL	HIGH	MEDIUM	LOW	INFO	Total
Windows Application Assessment Vulnerabilities	0	0	0	0	1	1
Total	0	0	0	0	1	1

3.2 Summary of Vulnerabilities Found

Windows Application Assessment Vulnerabilities

Severity Level	Vulnerability Name	Issue Status
INFORMATIONAL	Insecure Function Used	CLOSED

4 Windows Application Assessment Vulnerabilities

Insecure Functions Used

Windows Application	INFORMATIONAL
Issue Status	CLOSED

The lightway application's source code was observed to utilise insecure C and C++ functions which does not safely validate the input parameters (i.e. does not perform bounds checking). However, it was confirmed that the usage of these functions was not exploitable because manual buffer size checks, guaranteed sizes and proper null termination were implemented. This issue was raised as deviation from best practices.

Retest (2022-04-13)

During the retest, the affected functions in the source code were either replaced with function that safely validate parameters or were removed. Hence, this issue was deemed to be sufficiently remediated, and has been marked as 'Closed'.



F-Secure®