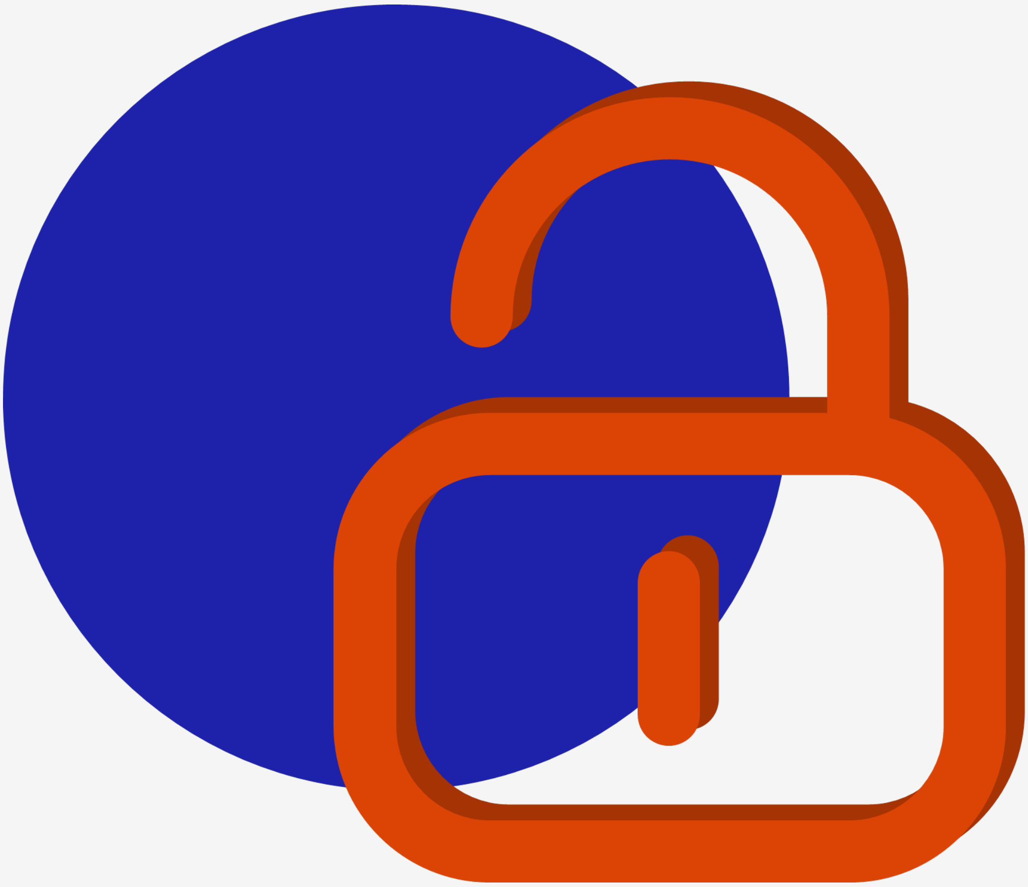
++

Sophos Connect Client Security Review: Letter of Attestation

Sophos

28 November 2024



Document Control

Date	Change By	Change	Issue
2024–11–07	Christo Erasmus	Document created	0.1
2024–11–28	Christopher Panayi	Document published	1.0

Document Distribution

Date	Name	Company
2024–11–28	Steven Hedworth	Sophos

Contents

1. Overview

MWR CyberSec (MWR) conducted a security assessment of the Sophos Connect VPN client, on both the macOS and Windows platforms. This assessment was conducted from the 27th of September to the 6th of November 2024, in conjunction with a security review of specific components of the Sophos Firewall.

The assessment aimed to identify vulnerabilities in the Sophos Connect client that could undermine the security of the machines it is installed on, or result in the exposure of sensitive information, such VPN credentials and secrets.

2. Approach

The Sophos Connect client made use of open-source VPN libraries for establishing VPN connections, and this assessment focused on the aspects of the Connect client that were developed by Sophos, as well as its integration with (and configuration of) the open-source libraries.

The assessment followed a white-box approach, with the MWR testing team being given access to source code, documentation and the development team, where relevant. All components of the Connect client were considered in-scope, and the following high-level areas were prioritised:

- Retrieval or tampering of sensitive data by low-privileged users
- Various inter-process communication mechanisms employed by the Sophos Connect client
- The use of operating system mechanisms to protect the Sophos Connect client and its various components
- Integration and configuration of external libraries
- Specific functionality in the Sophos Connect client that could potentially be used to attack the device it is running on

3. Results

Assessment	HIGH	MEDIUM	LOW	INFORMATIONAL
Sophos Connect Client Security Review	0	2	1	5
Total	0	2	1	5

The Sophos Connect client was considered to have a good security posture, as the majority of the vulnerabilities that were identified did not pose a significant risk. Attacks that exploited the identified medium risk vulnerabilities were considered to be complex to perform and could not directly result in privilege escalation.

Recommendations on remediating the identified vulnerabilities, architectural considerations and mechanisms for further hardening were provided for the Windows and macOS client implementations. The Sophos Connect team was receptive to findings and remedial actions, as well as being highly responsive and interactive throughout the course of the engagement.

Risk Rating Scale

The following risk profiles were used as guidelines to classify the vulnerabilities:

HIGH	A vulnerability will be assessed as representing a high risk if it holds the potential for an attacker to control, alter or delete Sophos' electronic assets. For example, a vulnerability which could allow an attacker to gain unauthorised access to a system or to sensitive data would be assessed as a high risk. Such issues could ultimately result in the defacement of a web site, the alteration of data held within a database or the capture of sensitive information such as account credentials or credit card information.
MEDIUM	A vulnerability will be assessed to represent a medium risk if it holds, when combined with other factors or issues, the potential for an attacker to control, alter or delete Sophos' electronic assets. For example, a vulnerability that could enable unauthorised access to be gained if a specific condition was met, or an unexpected change in configuration was to occur, would be rated as a medium risk.
LOW	A vulnerability will be assessed to represent a low risk if the likelihood or impact of exploitation is extremely low. For example, this could be an HTTPS configuration that allows weak ciphers or outdated protocols, or a CAPTCHA that can be solved programmatically.
INFORMATIONAL	A vulnerability will be assigned the informational classification when it cannot be exploited directly but is not in line with security best practice. Such a vulnerability could provide information that would facilitate research into an attack against the target system. For example, disclosure of the server type in an HTTP response.

APPENDIX I – Project Team

Assessment Team

Lead Consultant	Christopher Panayi
Additional Consultants	Christo Erasmus Connor du Plooy

Quality Assurance

QA Consultants	Momelezi Mchunu Johan van der Merwe Matthew Bouffé Mohammad Pathan Stephen Munro

Project Management

Delivery Manager	Catherine de Wet
Account Director	Gaylen Postiglioni

MWR

CYBERSEC