++

Endpoint Solutions Security Assessment: Attestation Letter

Sophos

19 January 2023

Document Control

Date	Change By	Change	Issue
2023–01–19	Pierre Kleynhans	Document created	0.1
2023–01–19	Tinus Green	Document QA	0.2
2023–01–19	Pierre Kleynhans	Document published	1.0

Document Distribution

Date	Name	Company
2022–01–19	Steven Hedworth	Sophos

Contents

1. Overview

MWR CyberSec (MWR) was commissioned by Sophos to perform an in-depth security assessment of their Sophos Endpoint Protection solution for Windows and macOS, and the Sophos Server Protection solution for Linux. The assessment was performed from the 26th of September to the 15th of December 2022. The goal of this engagement was to identify potential security weaknesses within each agent that could be detrimental to the security posture of devices that made use of Sophos endpoint protection products.

MWR's consultancy team has built an enviable reputation as a research-driven cyber security consultancy firm. The team has a proven track record of collaborating with organisations that are industry leaders in information security. Beyond the technical competency of consultants, MWR prides itself in providing a unique set of client engagement services that put security management at the core of clients' business processes. Consultants are experienced in analysing the security architecture of solutions and providing catered security design recommendations.

2. Approach

Multiple components that formed part of each Sophos Endpoint Protection solution were considered in scope for this engagement, which were part of the following platforms:

- Sophos Endpoint Protection for Windows
- Sophos Server Protection for Linux
- Sophos Endpoint Protection for macOS

Each platform's protection solution was assessed to identify security weaknesses in the agents' default configuration, and to discover potential vulnerabilities that could be exploited in a manner that exposed the affected devices to cyber security risks. This included an in-depth assessment of the various components making up each endpoint agent, inter-process communication between these components, as well as network communication between the agents and Sophos Central.

Focus was placed on testing for vulnerabilities that could be used by an attacker to achieve possibly unforeseen risks, such as escalating privileges on the underlying host or completely disabling the agent. The assessment was performed using a white box approach, with access to architecture details and source code.

3. Results

The table below shows a summary of the results and their corresponding risk ratings:

High	Medium	Low	Informational
1	4	6	11

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 abuse the endpoint agent to escalate privileges on the underlying host, or to disable critical functionality of the agent.
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 abuse the endpoint agent to escalate privileges on the underlying host, or to disable critical functionality of the agent. For example, a vulnerability that could enable an attacker to disable the agent 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 a TLS configuration that allows weak ciphers or outdated protocols.
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.

It was clear that Sophos developed each solution with security in mind, as indicated by the vast majority of findings being classified as low or informational risk. No vulnerabilities were found that could be used to facilitate privilege escalation on the underlying host. The one high risk finding was isolated to the macOS endpoint agent.

APPENDIX I – Disclaimer and Non-Disclosure Agreement

Non-Disclosure Statement

This report is the sole property of Sophos. All information obtained during the testing process is deemed privileged information and not for public dissemination. MWR CyberSec pledges its commitment that this information will remain strictly confidential. It will not be discussed or disclosed to any third party without the express written consent of Sophos. MWR CyberSec strives to maintain the highest level of ethical standards in its business practice.

Non-Disclosure Agreement

MWR CyberSec and Sophos have signed an NDA.

Disclaimer

This report is not meant as an exhaustive analysis of the level of security now present on the tested hosts, and the data shown here should not be used alone to judge security of any computer system. Some scans were performed automatically and may not reveal all the possible security holes present in the system. Some vulnerabilities that were found may be 'false positives', although reasonable attempts have been made to minimise that possibility. In accordance with the terms and conditions of the original quotation, in no event shall MWR CyberSec or its employees or representatives be liable for any damages whatsoever including direct, indirect, incidental, consequential loss or other damages.

APPENDIX II – Project Team

Assessment Team

Lead Consultant	Warren Arthur
Additional Consultants	Kyle Prinsloo Colman Mbuya Pierre Kleynhans Shezad Mia Connor Du Plooy

Quality Assurance

QA Consultants	Shezad Mia Pierre Kleynhans Christopher Panayi Kevin Musengi

Project Management

Delivery Manager	Carla Watermeyer
Account Director	Gaylen Postiglioni

MWR CYBERSEC