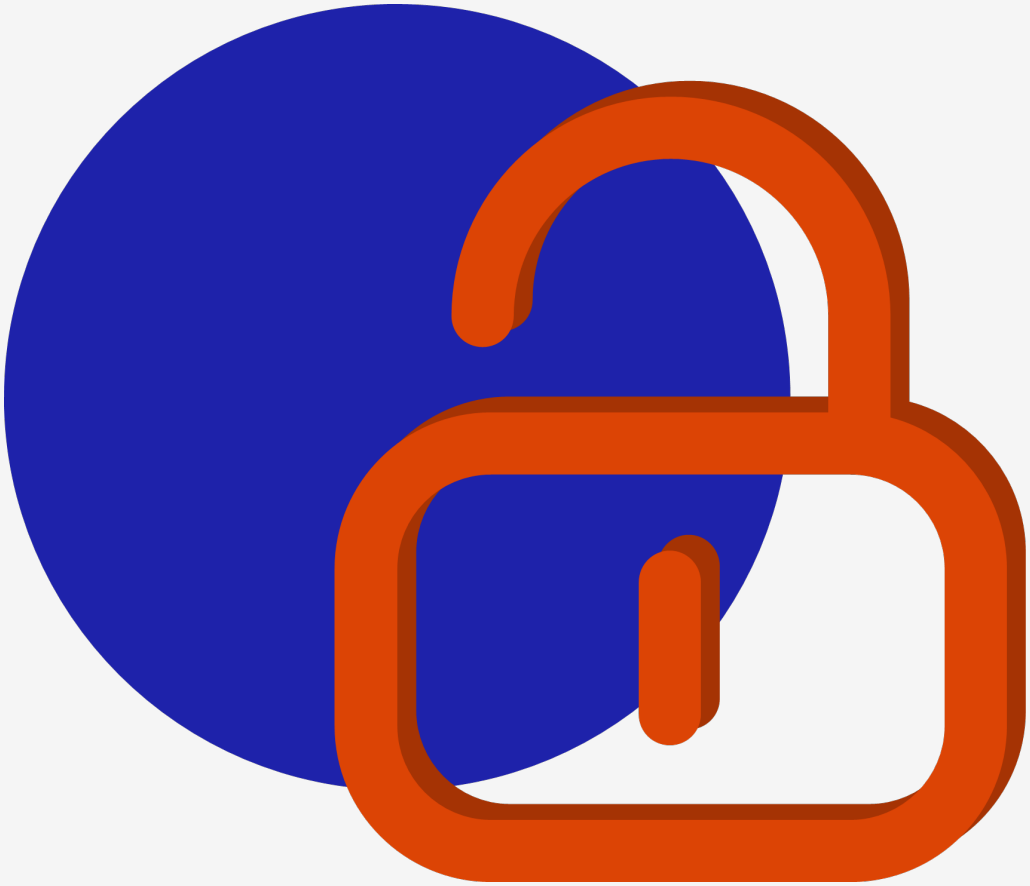
++

Sophos Endpoint Security Assessment: Letter of Attestation

Sophos

4 October 2024



MWR CYBERSEC

Document Control

Date	Change By	Change	Issue
2024–08–30	Christo Erasmus	Document created	0.1
2024–09–10	Logan Kroeger	Document amended	0.2
2024–09–10	Matthew Bouffé	Document QA	0.3
2024–10–01	Connor du Plooy	Document amended	0.4
2024–10–02	Gladwin Mohlamonyane	Document amended	0.5
2024–10–02	Momelezi Mchunu	Document QA	0.6
2024–10–02	Kevin Musengi	Document QA	0.7
2024–10–04	Christopher Panayi	Document published	1.0

Document Distribution

Date	Name	Company
2024–10–04	Steven Hedworth	Sophos

Contents

1. Overview

MWR CyberSec (MWR) conducted several security assessments against Sophos' endpoint security solutions for various Operating systems. The platforms that were included in this assessment, as well as the specific components that were considered in-scope, are as follows:

- Sophos Endpoint Protection for Windows
  - Scope:
    - Management Communication System (MCS)
    - Injection DLLs and IPC mechanisms
  - Date:
    - Conducted from the 1st of August to the 9th of September 2024
- Sophos Server Protection for Linux
  - Scope:
    - Device Isolation
    - Privilege Escalation Attack Vectors
  - Date:
    - Conducted from the 7th of August to the 12th of September 2024
- Sophos Endpoint Protection for macOS
  - Scope:
    - Enhanced tamper protection
    - Sophos Detection (file interception scanning process)
    - General fuzzing
  - Date:
    - Conducted from the 22nd of August to the 26th of September 2024

2. Approach

The sections below details the high-level approach taken for the endpoint agent against each platform.

2.1. Windows

The assessment of the Windows MCS component focused on the integrity of the TLS communications between the agent and the Sophos Central platform, as well as determining whether it was possible to gain unauthorised access to the API and use its functionality to impact the security of the endpoint. Additionally, the storage of secrets and sensitive information, mechanisms used by MCS to communicate with other components of the agent, and the management of configuration settings were also assessed. Finally, the assessment considered any changes introduced to Windows by the Sophos agent (focusing on MCS), as well as its ongoing behaviour at runtime, that could potentially be leveraged to compromise the security of the endpoint or the agent.

The assessment of the injection DLLs and IPC mechanisms focused on identifying any vulnerabilities that could degrade the overall security of the endpoint that the Sophos agent was installed on. Testing of the DLLs included, but was not limited to, the static analysis of the DLLs, the injection mechanisms utilised, and exported functions exposed. For the IPC mechanisms, testing was conducted against each of the different IPC mechanisms utilised by the injection DLLs. Finally, a time-boxed approach was taken for investigating any other potential findings encountered during the assessment of the injection DLLs and IPC mechanisms.

2.2. Linux

The assessment of the Linux component focused on the identification of privilege escalation vectors that the solution may introduce to the endpoint that it was installed on. Additionally, the agent's ability to effectively isolate the endpoint through its Device Isolation feature was investigated.

2.2.1. Device Isolation

The solution's device isolation functionality was facilitated by a software component that used the netfilter project's `nftables`[1]. The solution was triggered to enable firewall rules when Device Isolation was enabled on Sophos Central. Additionally, it had functionality to incorporate exclusions to its isolation rules based on configurations that were set on the Central dashboard.

A dynamic and static testing approach was taken to identify weaknesses in the solution's implementation. This allowed for robust test cases to be explored through the correlation of what could be seen in the application's source code and observations made against the application while performing dynamic instrumentation.

2.2.2. Privilege Escalation

The approach taken to explore this risk was similar to how device isolation was tested; however, additional threat modelling sessions were held with the development team to further explore specific aspects of the overall solution's implementation.

2.3. macOS

The approach to testing consisted of a combination of static and dynamic analysis techniques, which were applied after threat modelling sessions with the Sophos teams. Potential vulnerabilities were checked for using a device that had the endpoint protection agent installed, but System Integrity Protection (SIP) disabled, to enable instrumentation of the endpoint agent. Specific focus was placed on finding vulnerabilities that would allow malicious software to bypass tamper protection, evade Sophos Detection or any vulnerabilities that would degrade the security of the endpoint. All findings were verified on a system with SIP enabled, to ensure accurate results.

Testing time was reallocated from the general fuzzing component to other testing components to ensure the thoroughness of the test cases performed and potential improvements in the internal testing of the agent were provided in the assessment report.

[1] https://nftables.org/

3. Results

Assessment	HIGH	MEDIUM	LOW	INFORMATIONAL
Linux Endpoint Security Assessment	1	1	1	0
macOS Endpoint Security Assessment	1	2	4	2
Windows Endpoint Security Assessment	0	1	4	1
Total	2	4	9	3

The endpoint security agents were considered to have a good security posture, as the majority of findings were either low risk or informational in nature. Analysis of the source code and technical verification of potential vulnerabilities indicated that Sophos had created the solutions while considering the security implications of decisions taken.

Platform-Specific Commentary

Windows agent

The majority of findings for the Windows component were considered to be low risk or informational in nature. One medium risk vulnerability was discovered, however this required administrative rights on the machine to exploit.

Linux agent

Through the test cases performed against the Linux endpoint agent, it was observed to be well implemented with a strong focus on the Unix permissions applied to both its files and Unix sockets. This reduced the attack surface exposed to threat actors who may have gained access to the host.

Testing did result in the identification of a high-risk vulnerability, which was not found to affect the security of the endpoint agent itself. Other findings that were made against the solution were assigned a medium and low-risk rating due to the requirement of needing administrative rights for their exploitation.

macOS agent

For the identified high risk finding on macOS, remediation was expected to require limited effort, as the majority of work towards remediating this finding had already been done at the time of discovery.

Overall Test Impressions

Recommendations on remediating the identified vulnerabilities and mechanisms for further hardening of the endpoint agents have been made across all three platforms. The Sophos 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 Gladwin Mohlamonyane Jacob Simmons Logan Kroeger

Quality Assurance

QA Consultants	Matthew Bouffé Momelezi Mchunu Kevin Musengi

Project Management

Delivery Manager	Catherine de Wet
Account Director	Gaylen Postglioni

MWR CYBERSEC