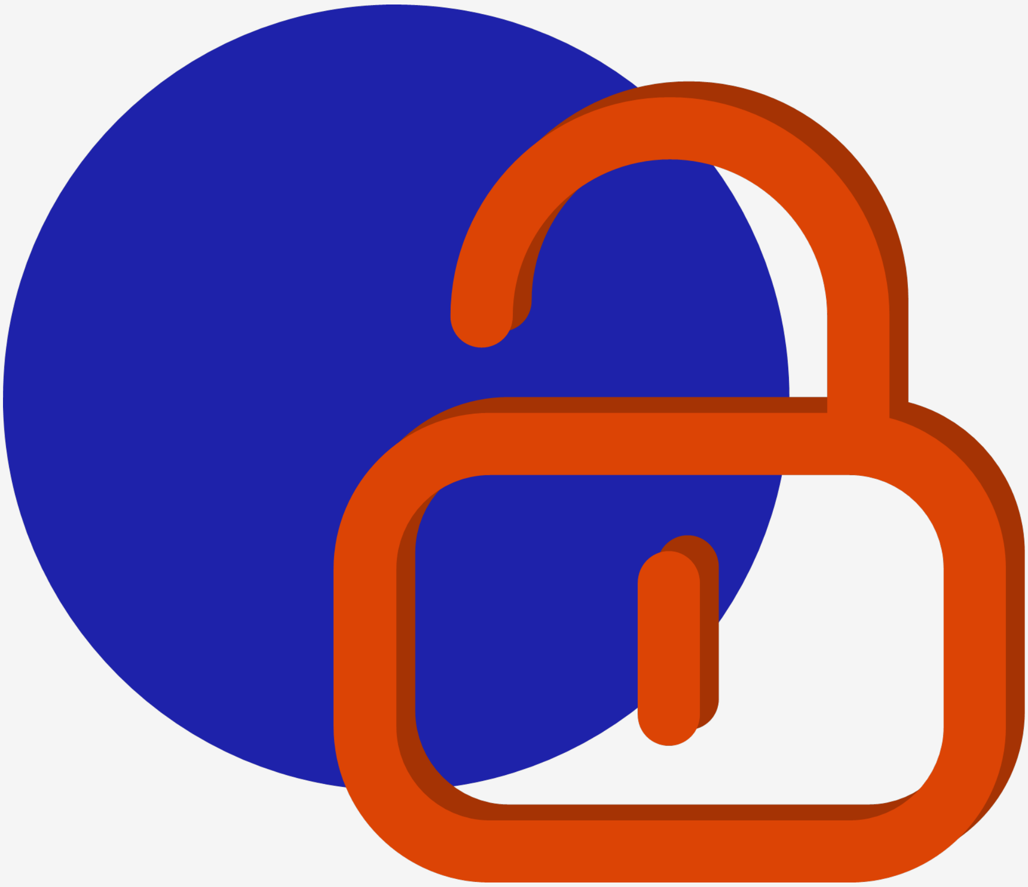
Sophos SMC Assessment

Sophos

23 August 2024



Document Control

Date	Change By	Change	Issue
2024–08–06	Tswelopele Moshe	Document created	0.1
2024–08–22	Kevin Musengi	Document QA	0.2
2024–08–23	Tswelopele Moshe	Document published	1.0

Document Distribution

Date	Name	Company
2024–08–23	Steven Hedworth	Sophos
2024–08–23	Sam Caise	Sophos

Contents

1. Overview

MWR CyberSec (MWR) conducted a security assessment of Sophos' key components of the Central-integrated Sophos Mobile Control (SMC) solution. SMC was a mobile device management solution that was used by organisations to provide security to mobile devices through centralised configuration and application deployment. The assessment was conducted remotely from the 6th of August 2024 to the 22nd of August 2024. For this assessment, key components and features of the SMC were assessed to ensure that no vulnerabilities were present. These components were the following:

- Sophos Mobile Control Web Application Best Effort Assessment
  - An assessment of the administrative interface for Sophos Mobile. This interface allowed customers to manage endpoint devices and perform various administrative actions.
- Sophos Central to Sophos Mobile Control SSO Integration Best Effort Assessment
  - An assessment of the authentication code and logic flow for the custom Single-Sign On (SSO) solution for the SMC administration panel.
- Sophos Mobile API Web Services Assessment
  - An assessment of the `smc-xdr-netlog`, `azure-svc-locator`, and the `mobile-api` endpoints.

2. Approach

A strong emphasis was placed on testing for authentication and authorisation-related vulnerabilities as well as any security gaps which may arise as a consequence of insufficient input validation. On the web services and web application portions of the assessment, common web-based vulnerabilities aligned with OWASP Top 10, such as injection attacks, code-execution vectors, and logic flaws were tested for.

This assessment included a separate component to ensure that the SSO integration between Central and Sophos Mobile was secure and could not be exploited. All three components of the assessment were code-assisted, therefore auditing the code for outdated or insecurely-used dependencies was part of this assessment.

3. Results

Assessment	HIGH	MEDIUM	LOW	INFORMATIONAL
Web Application Assessment	0	0	2	3
Web Services Assessment	0	0	0	1
Total	0	0	2	4

As seen above, a total of two low-risk vulnerabilities as well as four informational-risk vulnerabilities were identified within the web application and web services components, while no vulnerabilities were identified in the SSO Integration assessment. The security posture of all three in-scope components were found to be of a good security standard, as no vulnerabilities were identified that could be exploited to directly attack Sophos or it's customers. However, recommendations surrounding input validation on the Sophos Mobile Control web application should be considered and implemented to further strengthen the existing security controls.

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's 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's 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 – 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	Robin Roodt
Additional Consultants	Nick Brown Tswelopele Moshe

Quality Assurance

QA Consultant	Kevin Musengi

Project Management

Delivery Manager	Catherine de Wet
Account Director	Gaylen Postiglioni

MWR CYBERSEC